Rapport d'activités 2021
Activiteitenverslag 2021

Comité Permanent R
Vast Comité I

Comité Permanent de Contrôle des
services de renseignement et de sécurité

Vast Comité van Toezicht op
de inlichtingen- en veiligheidsdiensten

RAPPORT D'ACTIVITÉS 2021
ACTIVITEITENVERSLAG 2021

Quis custodiet ipsos custodes ?

Quis custodiet ipsos custodes ? est une série de publications qui a pour objectif de stimuler une discussion approfondie sur le fonctionnement, les compétences et le contrôle des services de renseignement et de sécurité et sur le travail de renseignement. Dans cette série figurent notamment des études scientifiques, les rapports d'activités du Comité permanent R et des rapports de colloques.

Rédaction

Comité permanent de Contrôle des services de renseignement et de sécurité, rue de Louvain 48, boîte 4 à 1000 Bruxelles (02 286 29 88).

Déjà parus dans cette série

1) D. Van Daele, en B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Comité permanent R, *Rapport d'activités 2006,* 2007, 147 p.
3) Comité permanent R, *Rapport d'activités 2007,* 2008, 87 p.
4) Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight against Terrorism - Fusion Centres throughout Europe*, 2010, 220 p.
5) Comité permanent R, *Rapport d'activités 2008,* 2009, 131 p.
6) W. Van Laethem, D. Van Daele en B. Vangeebergen (eds.), *De Wet op de bijzondere inlichtingenmethoden,* 2010, 298 p.
7) Comité permanent R, *Rapport d'activités 2009,* 2010, 127 p.
8) Comité permanent R, *Rapport d'activités 2010,* 2011, 119 p.
9) Comité permanent R, *Rapport d'activités 2011,* 2012, 134 p.
10) W. Van Laethem et J. Vanderborght, *Regards sur le contrôle. Vingt ans de contrôle démocratique sur les services de renseignement*, 2013, 565 p.
11) Comité permanent R, *Rapport d'activités 2012*, 2013, 127 p.
12) Comité permanent R, *Rapport d'activités 2013*, 2014, 212 p.
13) Comité permanent R, *Rapport d'activités 2014*, 2015, 141 p.
14) Comité permanent R, *Rapport d'activités 2015*, 2016, 131 p.
15) Comité permanent R, *Rapport d'activités 2016*, 2017, 227 p.
16) Comité permanent R, *Rapport d'activités 2017*, 2018, 152 p.
17) Comité permanent R, *Rapport d'activités 2018*, 2019, 167 p.
18) J. Vanderborght (ed.), *Les méthodes particulières de renseignement : de l'ombre à la lumière*, 2019, 151 p.
19) Comité permanent R, *Rapport d'activités 2019*, 2020, 148 p.
20) Comité permanent R, *Rapport d'activités 2020*, 2021, 189 p.
21) Comité permanent R, *Rapport d'activités 2021*, 2022, 241 p.

RAPPORT D'ACTIVITÉS 2021

Comité permanent de Contrôle des services de renseignement et de sécurité

Comité permanent de Contrôle des services
de renseignement et de sécurité

Le présent Rapport d'activités 2021 a été approuvé par le Comité permanent de Contrôle des services de renseignement et de sécurité lors de la réunion du 25 mai 2022.

(soussignés)
Serge Lipszyc, président
Pieter-Alexander De Brock, conseiller
Thibaut Vandamme, conseiller
Frédéric Givron, greffier

Rapport d'activités 2021
Comité permanent de Contrôle des services de renseignement et de sécurité

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

AC(C)	Autorité de contrôle (compétente)
AG	Administrateur général (VSSE)
AIVD	*Algemene Inlichtingen- en Veiligheidsdiensten*
A.M.	Arrêté ministériel
Ann. parl.	Annales parlementaires
ANS	Autorité nationale de sécurité
APD	Autorité de protection des données
A.R.	Arrêté royal
AR BDC	Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters et portant exécution de certaines dispositions de la section 1er*bis* « de la gestion des informations » du chapitre IV de la loi sur la fonction de police
AR C&HS	Arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité
AR FTF	Arrêté royal du 21 juillet 2016 relatif à la banque de données commune 'Foreign Terrorist Fighters' et portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police
AR OCAM	Arrêté royal du 28 novembre 2006 portant exécution de la Loi du 10 juillet 2006 relative à l'analyse de la menace
AR PH	Arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police
AR TF	Arrêté royal du 23 avril 2018 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police et modifiant la banque de données commune Foreign Terrorist Fighters vers la banque de données commune Terrorist Fighters

A-Rens	Autorité de surveillance indépendante des activités de renseignement
BCP	*Business continuity plan*
BDC	Banques de données communes
BDC PH	Banque de données commune ' Propagandistes de haine'
BDC TF	Banque de données commune ' Terrorist fighters'
BELPIU	*Belgian Passenger Information Unit* (Unité belge d'information des passagers)
BfV	*Bundesamt für Verfassungsschutz*
BINII	*Belgian Intelligence Network Information Infrastructure*
BNG	Banque de données nationale générale
CAC	Cellule administrative de coordination
CaMa	*Case Managers (*SGRS)
CCB	Centre pour la Cybersécurité Belgique
CCIRM	*Collection Coordination Information Requirement Management* (SGRS)
CCL	Conseil Central Laïque
CCRS	Comité de coordination du renseignement et de la sécurité
CE	Contre-extrémisme
CEDH	Convention européenne des droits de l'homme
CelEx	Cellule Extrémisme (SPF Justice)
CI	*Counterintelligence*
CIA (model)	Confidentiality, Integrity & Availability (model)
CIAOSN	Centre d'information et d'avis sur les organisations sectaires nuisibles
CJUE	Cour de justice de l'Union européenne
CM BDC	Circulaire du 22 mai 2018 du Ministre de la Sécurité et de l'Intérieur et du Ministre de la Justice relative à l'échange d'informations et au suivi des Terrorist Fighters et des Propagandistes de haine
CMDB	*Component Management DataBase* (base de données de gestion de configuration)
CMOJ	Commission de Modernisation de l'Ordre judiciaire
CNS	Conseil national de sécurité
Cour EDH	Cour européenne des droits de l'homme
C.O.C.	Organe de contrôle de l'information policière
CoMa	*Collection Managers* (SGRS)
Comité permanent P	Comité permanent de Contrôle des services de police
Comité permanent R	Comité permanent de Contrôle des services de renseignement et de sécurité

Commission BIM	Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité
CRABV	Compte Rendu Analytique – *Beknopt Verslag*
CRIV	Compte Rendu Intégral – *Integraal Verslag*
CSIL-R	Cellule de Sécurité Intégrale Locale - Radicalisme
CTIF	Cellule de Traitement des Informations Financières
CTIVD	*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten*
DG EPI	Direction générale des Établissements Pénitentiaires (SPF Justice)
DGSP	Direction générale Sécurité & Prévention (SPF Intérieur)
DISCC	*Defense Intelligence and Security Coordination Centre* (SGRS)
DJSOC/Terro	Direction de la lutte contre la criminalité grave et organisée (section terrorisme) de la Police judiciaire fédérale
Doc. parl.	Documents parlementaires de la Chambre et du Sénat
DPA	*Data Protection Authority*
DPO	*Data Protection Officer*
DRI	Direction de l'information policière et des moyens ICT (Police fédérale)
DRP	*Disaster recovery plan*
EPV	Extrémiste potentiellement violent
ERM	École Royale Militaire
FTF	*Foreign terrorist fighters*
GEOINT	*Geospacial intellingence*
HTF	*Homegrown terrorist fighters*
HUMINT	*Human intelligence*
ICM	*Incident & Crisis Management*
ICT	*Information and communications technology*
IEFH	Institut pour l'égalité entre les femmes et les hommes
IFDH	Institut fédéral pour la protection et la promotion des droits humains
IOWG	*Intelligence Oversight Working Group*
IPCO	*Investigatory Powers Commissioner's Office*
JDC	*Joint Decision Centre*
JIC	*Joint Intelligence Centre*
LCE	Loi du 13 juin 2005 relative aux communications électroniques
L.Contrôle	Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace

L.C&HS	Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité
LFP	Loi du 5 août 1992 sur la fonction de police
L.OCAM	Loi du 10 juillet 2006 relative à l'analyse de la menace
Loi APD	Loi du 3 décembre 2017 portant création de l'Autorité de protection des données
Loi MRD	Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité
Loi PNR	Loi du 25 décembre 2016 relative au traitement des données des passagers
L.Org.recours	Loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité
LPA	Loi du 11 avril 1994 relative à la publicité de l'administration
LPD	Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (Loi Protection des données)
L.R&S	Loi du 30 novembre 1998 organique des services de renseignement et de sécurité
LTF	*Local task force*
M.B.	Moniteur belge
MoU	*Memorandum of Understanding*
MPLUS	Méthodes ordinaires plus
MRD	Méthodes de recueil des données
NA	Note aux autorités
NTSU-CTIF	*National Technical & Tactical Support Unit – Central Technical Interception Facility* (Police intégrée)
OCAM	Organe de coordination pour l'analyse de la menace
OE	Office des étrangers
OSINT	*Open sources intelligence*
OTAN	Organisation du Traité de l'Atlantique Nord
PCT	Personnes condamnées pour terrorisme
PDT-IA	Cellule *Pre-Deployment Training for Individual Augmentees* (Défense)
PH	Propagandistes de haine
Plan R	Plan d'action Radicalisme
Plateforme CT	Plateforme commune contre-terrorisme
PROTEUS	Banque de données de l'OCAM
PSNR	Plan Stratégique National du Renseignement
Q. et R.	Questions et réponses écrites (Chambre ou Sénat)

RFC	*Requests for Collect*
RFI	*Request for information*
RGPD	Règlement Général sur la Protection des Données
SARM	Service d'assistance religieuse et morale (Défense)
SGRS	Service Général du Renseignement et de la Sécurité
SIGINT	*Signal intelligence*
SOP	*Standard Operating Procedures*
SPF	Service public fédéral
TF	*Terrorist fighters*
VSSE	Sûreté de l'État

PRÉFACE

L'année 2021 nous a rappelé à quel point la planète était vulnérable, à quel point les sociétés étaient fragilisées, à quel point la démocratie était remise en question, à quel point les droits des citoyens étaient précaires.

Le phénomène des extrémistes potentiellement violents – religieux ou idéologiques – s'est amplifié par des attaques contre les institutions et a affaibli durablement celles-ci. L'assaut du Capitole à Washington est certainement l'exemple le plus révélateur du rejet des institutions démocratiques. Un tel scenario ne pourrait-il pas toucher nos institutions belges ?

Ce type de menace, loin de disparaître, a été, au contraire, renforcée par les médias sociaux. C'est ainsi que de nombreuses théories conspirationnistes autour de la COVID-19 ont été propagées. Même si le terreau était déjà présent, la pandémie s'est avérée être le parfait prétexte pour dresser davantage des groupes de population les uns contre les autres.

Aujourd'hui comme hier, les coups d'État, les renversements des 'pouvoirs en place' nous obligent à intervenir et à rapatrier si nécessaire nos compatriotes. Cette volonté de protéger nécessite le renforcement de l'engagement de nos services de renseignement et de sécurité à l'étranger.

Le procès à la suite des attentats de Paris, tout comme le procès d'Anvers suite à l'attentat déjoué de Villepinte, nous rappelle également la nécessité pour les services de renseignement de renforcer leur partenariat et de renforcer la lutte commune contre le terrorisme.

En Belgique, les problématiques liées aux mouvements djihadistes ont servi de terreau fertile à la polarisation croissante de la société. Le rapport d'enquête sur le suivi de l'extrême droite a lui aussi montré sa pertinence. À la suite de la traque d'un militaire armé, menaçant nos institutions, l'enquête du Comité a mis en évidence la fragilité de certaines de nos institutions face à ce phénomène qui ne touche plus seulement nos pays voisins.

En ce qui concerne nos services de renseignement, rappelons que notre pays est un carrefour pour de nombreuses institutions européennes et internationales ainsi que de nombreuses communautés et d'opposants. Cette situation particulière exige un investissement permanent dans le renforcement de la protection de ses acteurs et dans la lutte contre les ingérences étrangères.

Il faut encourager les services de la sécurité à agir de manière plus proactive et de mieux interagir entre eux, en visant ainsi une communauté belge du renseignement et de la sécurité consolidée et soudée. J'appuie Jaak Raes, l'Administrateur général de la Sûreté de l'Etat, dans sa volonté de voir dorénavant le « besoin de savoir » (need to know) se concilier avec le « besoin de partager » (need to share).

Je soutiens le projet de statut unique des personnels des services de renseignement et de sécurité. Il est assurément un pas indispensable dans le développement des synergies entre services. J'invite à l'optimisation des ressources ainsi qu'au renforcement de l'expertise disponible dans la lutte contre les menaces. Je pense que la question de la sécurité nécessite une vision stratégique plus claire et ambitieuse du Conseil national de sécurité sur les enjeux de sécurité qui nous sont imposés par l'évolution de notre société.

En raison des impacts du COVID-19, l'organisation quotidienne du Comité a été profondément bouleversée. Il n'a été possible de garantir la continuité du travail que grâce à la conscience professionnelle tenace de chacun.e. Nos collaborateurs ont d'autant plus de mérite qu'ils n'ont pu que très partiellement recourir au télétravail. Nous manquons toujours d'un indispensable réseau digitalisé sécurisé qui nous fait défaut dans nos tâches au quotidien. Et si les défis sont nombreux, le Comité entend y répondre avec pertinence.

Le chantier nécessaire des synergies ouvert par la Chambre permet enfin, aujourd'hui, d'en entrevoir les fondations. Il suscite encore logiquement bon nombre de questions, d'inquiétudes mais aussi d'espoirs. Le renforcement de l'institution du Comité reste d'actualité tout comme les questions soulevées par l'ouverture de dossiers relatifs à l'utilisation de logiciels espions, au suivi d'un imam, au suivi des condamnés terroristes, etc. Même s'il n'est pas le seul, le Comité permanent R est un rempart essentiel de notre Etat de droit.

Cette année fut aussi l'année du départ de plusieurs de nos collaborateurs Martine, Josiane, Wouter, Charles, Ludo, Frank, Jean-Philippe & Christophe que je souhaite remercier pour leur implication.

J'espère que la lecture de ce rapport contribuera à une meilleure perception de nos travaux et vous souhaite une lecture stimulante !

25 mai 2022,
Serge Lipszyc,
Président du Comité permanent de Contrôle
des services de renseignement et de sécurité

CHAPITRE I.
LES ENQUÊTES DE CONTRÔLE

En 2021, le Comité permanent R a finalisé dix enquêtes de contrôle, dont trois conjointement avec le Comité permanent de contrôle des services de police. En complément, trois dossiers d'information ont été présentés devant la Commission parlementaire de suivi et sont également repris dans le présent chapitre (I.4, I.6 et I.7).

Diverses instances et personnes peuvent 'saisir' le Comité permanent R d'une enquête de contrôle : la Commission parlementaire de suivi, les ministres compétents, toute personne (morale) qui souhaite introduire une plainte ou faire une dénonciation, etc. Le Comité peut lui aussi prendre l'initiative d'ouvrir une enquête de contrôle. Ce fut le cas pour cinq des dix enquêtes finalisées en 2021. Quatre enquêtes ont été initiées par la Commission parlementaire de suivi, et une enquête a été effectuée à la demande de la ministre de la Défense. Le Comité a par ailleurs poursuivi sept enquêtes ouvertes en 2021 ou antérieurement. Une description succincte des enquêtes en cours figure au chapitre I.14. Les recommandations émises à l'issue des enquêtes de contrôle ont été regroupées au Chapitre XI.

Le Comité permanent R a reçu, au total, 75 plaintes ou dénonciations en 2021.[1] Après une brève pré-enquête et la vérification de plusieurs données objectives, le Comité a rejeté 23 plaintes ou dénonciations parce qu'elles étaient manifestement non fondées[2] (art. 34 de Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (L.Contrôle)), ou dans 28 cas, parce que le Comité n'était pas compétent pour en traiter les griefs. Dans ce dernier cas de figure, les plaignants ont été renvoyés, si possible, vers les instances compétentes (en l'occurrence, le Procureur du Roi de Bruxelles, le Comité permanent P ou encore l'Autorité de protection des données (APD)). 14 des 24 plaintes traitées ont pu être clôturées en 2021, 10 plaintes étaient toujours en cours de traitement début 2022. En 2021, 16 des 24 plaintes traitées l'ont été en tant que plaintes *Data Protection Authority* (DPA).[3]

---

1 Dans un premier temps, la recevabilité de la plainte est examinée. Elle est ensuite classée dans une catégorie ('ordinaire', plainte APD, plainte MRD, etc.). Dans le cas d'une problématique générale, le Comité peut décider d'ouvrir une enquête de contrôle, sinon l'enquête reste limitée à la plainte (une enquête relative à une plainte).

2 Le Comité reçoit encore toute une série de plaintes et dénonciations fantaisistes.

3 Voir 'V.6. Traitement des requêtes individuelles'.

I.1. LES SERVICES D'APPUI DE L'OCAM (SUIVI)

En juin 2020, le Comité permanent R a, conjointement avec le Comité permanent P, finalisé un enquête de contrôle sur les services d'appui de l'Organe de coordination pour l'analyse de la menace (OCAM).[4] Cette enquête portait sur quatre services d'appui : le Service public fédéral (SPF) Intérieur (Office des étrangers), le SPF Affaires étrangères, le SPF Mobilité et Transports et le SPF Finances (Administration générale des Douanes et Accises).[5] L'enquête visait à examiner les relations entre les services d'appui précités et l'OCAM en ce qui concerne la coopération et l'échange d'informations. Une attention particulière a été accordée à la légalité, à l'efficacité et à la coordination de cette coopération et de cet échange d'informations.

Afin d'informer la Commission parlementaire de suivi de l'état d'avancement de la mise en œuvre des recommandations formulées dans le cadre de cette enquête, les Comités permanents R et P ont ouvert une enquête de suivi début juin 2020.[6]

L'enquête initiale avait ainsi notamment démontré le respect, par le SPF Affaires étrangères et le SPF Intérieur (Office des étrangers), des règles de traitement et de conservation des documents classifiés ainsi que la bonne circulation de l'information entre ces services et l'OCAM.

Dans leur rapport, les Comités permanents R et P formulaient des recommandations exclusivement à l'encontre du SPF Finances (Administration générale des Douanes et Accises) qui a élaboré un plan d'action afin de répondre aux exigences liées à son statut de service d'appui. En réponse aux conclusions et recommandations générales du rapport, le SPF Mobilité et Transport a toutefois également cherché à améliorer l'efficacité de sa collaboration avec l'OCAM. Le rapport de l'enquête de suivi se concentrait donc sur les mesures respectivement mises en place par ces deux administrations.

I.1.1. SUIVI DES RECOMMANDATIONS PAR LES DOUANES ET ACCISES

En réponse aux deux recommandations spécifiques formulées dans le rapport d'enquête en 2020, l'Administration générale des Douanes et Accises du SPF Finances a mis en place un plan d'action. Au moment de clôturer l'enquête de suivi (début 2021), la plupart des mesures prévues dans le plan d'action étaient

4 Voir COMITÉ PERMANENT R, *Rapport d'activités 2020*, 2-11 ('I.1. Les services d'appui de l'OCAM').

5 Les services de police et de renseignement ont déjà fait l'objet d'une enquête de contrôle commune portant sur les services d'appui de l'OCAM. Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2010*, 45-46 ('II.12.6. Communication de renseignements à l'OCAM par les services d'appui') et plus en détail : COMITÉ PERMANENT R, *Rapport d'activités 2011*, 25-33 ('II.4. Les flux d'informations entre l'OCAM et ses services d'appui').

6 Les résultats de cette enquête ont été présentés à la Commission de suivi en avril 2021.

partiellement mises en œuvre. Certaines actions n'avaient toutefois pas encore pu être réalisées, notamment en raison de la crise sanitaire.

La première recommandation spécifique appelait à clarifier, en interne, les informations recueillies qui sont pertinentes pour l'OCAM. Une première mesure prévoit ainsi d'établir un plan de collecte d'informations sur la base d'indicateurs d'extrémisme et de terrorisme. Un travail de sensibilisation a également été entamé afin d'encourager le signalement et le partage d'informations. Des formations étaient prévues à cette fin, notamment sur les indices d'extrémisme et de terrorisme. L'administration des Douanes et Accises a également procédé à un inventaire des sources d'informations en interne (les informations recueillies lors des activités opérationnelles de l'Administration Opérations et de l'Administration Recherches ou enregistrées dans les bases de données internes). En mars 2021, l'administration n'avait toutefois toujours pas accès à la banque de données commune gérée par l'OCAM.

La seconde recommandation portait sur le respect des normes légales de conservation et de consultation des documents classifiés. Outre l'acquisition de nouveaux coffres-forts et la mise en place d'un registre complet des informations classifiées, un manuel sur le traitement des documents classifiés était préparé par l'officier de sécurité de l'administration. En outre, l'Administration Recherches a limité l'accès au local BINII (*Belgian Intelligence Network Information Infrastructure*, une plateforme de communication pour l'échange d'informations classifiées). Le plan d'action prévoit également une vérification périodique des habilitations de sécurité ainsi que l'organisation de briefings de sécurité pour les titulaires d'habilitations.

Les Comités permanents P et R concluaient ainsi que l'Administration des Douanes et Accises a pris un certain nombre d'actions et de mesures nécessaires pour répondre aux recommandations formulées dans le rapport d'enquête initial.

I.1.2. SUIVI DES RECOMMANDATIONS PAR LE SPF MOBILITÉ ET TRANSPORTS

Malgré l'absence de recommandation spécifique à son encontre lors de l'enquête initiale, le SPF Mobilité et Transports a élaboré, lui aussi, un plan d'action, accompagné d'un calendrier, afin d'améliorer l'efficacité de sa coopération avec l'OCAM. Ce plan d'action visait, d'abord, à sensibiliser les collaborateurs aux missions de l'OCAM et aux échanges avec ce service. En 2020, plusieurs réunions ont ainsi été organisées par la Cellule de Crise du SPF Mobilité et Transports, tant en interne pour rappeler le rôle de l'OCAM et les objectifs de cette coopération qu'avec l'OCAM afin d'identifier les points d'amélioration et pistes d'action. En parallèle, au moment de clôturer l'enquête de suivi, un nouvel outil informatique était en cours de développement au sein du SPF Mobilité et Transports. Un tel outil devrait faciliter les échanges entre le SPF et l'OCAM et leur gestion.

Ensuite, le plan d'action prévoyait le développement et la mise en place de canaux privilégiés de partage d'informations en interne et vers l'extérieur. Dans ce cadre, un manuel de procédures quant à la gestion des documents classifiés et du système BINII a notamment été validé en interne.

Les effets de ces mesures ne pourront être évalués qu'avec le temps. Pour sa part, la Cellule de Crise du SPF regrettait toutefois à la clôture de l'enquête de suivi toujours le nombre encore trop important d'évaluations et d'informations en provenance de l'OCAM.

I.1.3. CONCLUSION

Tant le SPF Finances (Administration des Douanes et Accises) que le SPF Mobilité et Transports ont mis en place des plans d'action permettant de rencontrer les conclusions et recommandations formulées. Les Comités concluaient que ces différentes mesures devraient permettre de mieux garantir la sécurité des informations transmises, de faciliter le flux d'informations et d'avoir une meilleure connaissance de l'OCAM et de ses missions au sein de ces services d'appui.

I.2. L'OCAM ET LES SERVICES D'APPUI 'SUPPLÉMENTAIRES'

L'Arrêté royal (A.R.) du 17 août 2018 a élargi la liste des services d'appui de l'OCAM à quatre autres services, que sont la Direction générale Centre de crise, l'Administration générale de la Trésorerie, la Direction générale des Établissements pénitentiaires et le Service des cultes et de la laïcité de la Direction générale de la Législation et des Libertés et Droits fondamentaux du SPF Justice. Bien que cette décision remonte à août 2018, la première enquête[7] ne portait pas encore sur ces services, car il était prématuré d'effectuer une analyse du flux d'informations et des processus mis en œuvre dans ce cadre. Une nouvelle enquête de contrôle, menée conjointement avec le Comité permanent P, s'imposait.[8]

---

7 Voir COMITÉ PERMANENT R, *Rapport d'activités 2020*, 2-11 ('I.1. Les services d'appui de l'OCAM').

8 Les résultats ont été présentés à la Commission parlementaire de suivi en avril 2021.

I.2.1. LE FLUX D'INFORMATIONS

L'enquête visait à examiner les relations entre l'OCAM et les quatre services d'appui supplémentaires au regard de la transmission d'informations, de la légalité, de l'efficacité et de la coordination.

Une analyse quantitative des échanges offre un premier aperçu du flux d'informations entre les services d'appui et l'OCAM.

	2019				
	TOTAL	IN	OUT	RFI IN	RFI OUT
SPF JUSTICE – LAÏCITÉ ET CULTES	**13**	8	5	8	0
SPF JUSTICE – ÉTABLISSEMENTS PÉNITENTIAIRES	**2273**	2223	50	224	2
SPF FINANCES – ADMINISTRATION GÉNÉRALE DE LA TRÉSORERIE	**17**	14	3	7	0
SPF INTERIEUR – CENTRE DE CRISE	**2940**	1334	1606	7	8

Tableau 1 : Chiffres fournis par l'OCAM. Les données « IN » renvoient aux données entrantes à l'OCAM venant du service d'appui et les données « OUT » renvoient aux données sortantes de l'OCAM vers le service d'appui (Requests for Information (RFI) inclues).

Le tableau rend compte des informations échangées entre l'OCAM et les quatre services d'appui pour l'année 2019 selon les chiffres fournis par l'OCAM.[9] Ces données n'incluent pas les évaluations envoyées par l'OCAM, excepté pour le Centre de crise, premier destinataire des évaluations.

I.2.1.1. SPF Intérieur – Centre de crise

De par ses missions, le Centre de crise (à travers sa direction *Incident & Crisis Management* – ICM) est en contact permanent avec l'OCAM. En effet, le service définit les mesures à prendre sur la base des évaluations de la menace réalisées par l'OCAM. À ce titre, des réunions de coordination et de sécurité ont lieu très

[9] Ces données sont extraites de PROTEUS, la banque de données de l'OCAM. Il ne s'agit que des flux d'informations jugés pertinents par l'OCAM. Ces chiffres ne reprennent donc pas les échanges non encodés dans PROTEUS, par exemple des RFI envoyées à l'OCAM sur des entités inconnues.

fréquemment, et cela avant même que le Centre de crise ne soit désigné service d'appui.

Le flux d'informations de l'OCAM vers le Centre de crise est le plus important des quatre services d'appui supplémentaires et concerne pour la grande majorité des évaluations. En revanche, le Centre de crise ne fournit que très peu d'informations à l'OCAM, si ce n'est sur la tenue d'événements ou la venue de personnalités étrangères (par exemple par des demandes d'évaluations de la menace). La désignation comme service d'appui se justifie toutefois par la mise sur pied, au sein du Centre de crise, de l'Unité d'Information des Passagers (ou *Belgian Passenger Information Unit* – BELPIU).[10]

Étant donné les contacts permanents et la proximité de leurs bureaux, il n'y a pas de membres du personnel du Centre de crise détaché à l'OCAM. Le flux d'informations est décrit comme très bon par la Direction ICM. Les procédures mises en place, notamment l'utilisation des boites fonctionnelles, donnent des garanties contre les risques de perte d'informations.

L'échange d'informations se fait via trois canaux différents : par e-mail pour les informations et évaluations non classifiées ou en diffusion restreinte, par BINII pour les documents classifiés et par les Banques de données communes (BDC) que le Centre de crise peut interroger directement (*hit/no hit*). Les mesures de sécurité relatives aux documents classifiés sont respectées et appliquées par l'officier de sécurité.

I.2.1.2. SPF Justice – Direction générale des Établissements Pénitentiaires

Au sein de la Direction générale des Établissements pénitentiaires du SPF Justice, le point de contact de l'OCAM est la Cellule Extrémisme (CelEx), chargée du suivi des détenus signalés comme radicalisés.

Deux collaborateurs de CelEx sont détachés à l'OCAM comme experts. Ils participent ainsi aux missions de l'OCAM, par exemple dans le cadre du suivi et de l'évaluation de combattants terroristes étrangers, au sein du groupe de travail Prisons ou encore des *Local Task Force* (LTF). Ils ne sont par contre pas tenus au courant des changements potentiels au sein de la Direction générale des Établissements Pénintentiaires (DG EPI). Si CelEx ne voit pas la plus-value de ce détachement, perçu surtout comme une perte de capacité, l'OCAM apprécie en revanche l'expertise du milieu carcéral qu'apportent ces deux collaborateurs.

---

[10] L'Unité d'Information des Passagers collecte, enregistre et traite les données des passagers utilisant un transport international depuis, vers ou via la Belgique, tant à l'intérieur qu'à l'extérieur de l'Union européenne. Les données des passagers arrivent en continu des transporteurs et sont analysées sur la base de critères préalablement définis et confrontées aux banques de données BDC (Banques de Données Communes - OCAM) et BNG (Banque de données Nationale Générale - Police). Lorsque qu'il y a un « hit » en BDC (identités correspondantes), les informations sont encodées et envoyées notamment à l'OCAM. En outre, les données peuvent également faire l'objet de recherches ciblées.

Le flux d'informations avec la DG EPI se fait en grande majorité à destination de l'OCAM. La DG EPI fournit en effet un nombre important d'informations issues du réseau pénitentiaire à l'OCAM et, en retour, reçoit les évaluations des détenus. C'est également le service qui fait le plus de demandes d'informations (RFI) à l'organe de coordination.

L'accès aux BDC et leur alimentation facilitent ce flux d'informations. En outre, les routines de communication et de transmission mises en place (par e-mail via les boites fonctionnelles ou par porteur pour les documents classifiés) garantissent un bon fonctionnement.

CelEx doit toutefois gérer un flux important d'informations qui lui arrivent du réseau pénitentiaire. S'il dit ne pas manquer de personnel, le service souligne en revanche le besoin d'outils informatiques en appui à une meilleure gestion et à une meilleure analyse de toutes les informations qu'il reçoit.

Une permanence officielle serait également une plus-value non négligeable pour la DG EPI et ses différents partenaires.

I.2.1.3. SPF Finances – Administration générale de la Trésorerie

La coopération entre l'OCAM et l'Administration générale de la Trésorerie du SPF Finances s'inscrit uniquement dans le cadre du gel des avoirs des personnes liées au terrorisme.[11] La section Sanctions Financières du service *Compliance* au sein de la Trésorerie a été désignée point de contact à cette fin.

Le flux d'informations entre ce service d'appui et l'OCAM est quantitativement faible, ce qui peut s'expliquer par la spécificité de leur collaboration. De plus, il est très rare que l'Administration générale de la Trésorerie recueille des informations jugées pertinentes pour l'OCAM.

Un membre du personnel est détaché à l'OCAM depuis février 2019. Les procédures liées au gel des avoirs ne représentent toutefois que 20% de son temps de travail. Rattaché au département 'Appui stratégique - Communication' de l'OCAM, ce membre du personnel est en outre chargé de tâches administratives.

Les informations échangées avec la Trésorerie sont non classifiées. L'échange se fait essentiellement par e-mail via les boites fonctionnelles et professionnelles. Depuis fin 2020, la Trésorerie a en outre un accès direct aux BDC et une obligation de les alimenter. Une procédure interne a été élaborée par l'officier de sécurité en ce qui concerne l'accès et l'encodage dans les BDC.

---

11 Circulaire du 7 septembre 2015 relative à la mise en œuvre des articles 3 et 5 de l'A.R. du 28 décembre 2006 relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme – liste nationale.

I.2.1.4. SPF Justice – Direction générale de la Législation et des Libertés et Droits fondamentaux – Laïcité et Cultes

La désignation du Service des cultes et de la laïcité comme service d'appui de l'OCAM doit se lire au regard de ses compétences dans le cadre de la reconnaissance des cultes et organisations philosophiques non confessionnelles et de la gestion du statut des ministres du culte et représentants du Conseil Central Laïque (CCL). L'OCAM échange plus particulièrement avec la cellule « terrorisme et radicalisation » du service. Ce nouveau statut permet de légaliser le transfert d'informations, bien que le service ne récolte que peu d'informations pertinentes pour l'organe de coordination.

Une réunion a très vite été organisée entre l'OCAM et ce service d'appui supplémentaire afin de préciser les modalités de la coopération entre les deux services ainsi qu'entre le *Data Protection Officer* (DPO) et l'officier de sécurité du SPF Justice afin de mettre en place les accès ICT des BDC.

Le Service des cultes et de la laïcité a en effet accès aux BDC. Si le cadre légal prévoit uniquement un accès à la BDC Propagandistes de haine par interrogation directe (*hit/no hit*), il a été constaté que le service avait, en pratique, un accès complet aux BDC – qu'il juge utile et nécessaire. Le Comité a relevé l'importance de régulariser cet accès.[12]

Aucun membre du personnel n'a été détaché à l'OCAM, mais un collaborateur de l'organe de coordination a été désigné comme point de contact.

L'échange (restreint) d'informations se fait essentiellement par e-mail. Le service d'appui ne dispose toutefois pas d'une boite fonctionnelle : les e-mails sont par contre systématiquement adressés aux deux membres de la cellule « terrorisme et radicalisation » et au chef de service. Les documents classifiés seront transmis via le système BINII, désormais opérationnel au sein du SPF Justice, mais dans l'attente de l'élaboration de procédures internes pour son utilisation.

I.2.2. CONSTATATIONS ET CONCLUSION

Au terme de l'enquête, les Comités concluaient que les quatre services d'appui supplémentaires avaient identifié respectivement un point de contact pour leurs échanges avec l'OCAM qui centralise les informations échangées. Des membres du personnel sont détachés à l'OCAM pour la DG EPI (deux personnes) et la Trésorerie (une personne). Si la DG EPI y voit une perte de capacité, l'OCAM valorise l'expertise dont disposent ces collaborateurs.

12 Voir 'Chapitre V. Le contrôle des banques de données' ('V.2.3. de nouvelles recommndations').

L'échange d'informations est le plus important avec le Centre de crise et la DG EPI. En ce qui concerne la Trésorerie et le Services des cultes et de la laïcité, la collaboration avec l'OCAM reste très spécifique et restreinte à leurs compétences.

Tant L'OCAM que les services d'appui supplémentaires jugent l'échange d'informations entre eux comme étant très bon. Si des échanges avaient déjà lieu par le passé, la désignation comme service d'appui permet de légaliser cette collaboration, en particulier via les BDC. À travers son département gestion de dossiers/documentation, l'OCAM organise une permanence et dispose d'une boite fonctionnelle pour tous les échanges d'informations. À l'exception du Service des cultes et de la laïcité, ils disposent tous d'une boite fonctionnelle.

Les normes minimales de sécurité pour la conservation des documents classifiés sont respectées. La procédure pour l'utilisation du système BINII doit toutefois encore être finalisée pour le SPF Justice. Seule la Trésorerie n'échange pas d'informations classifiées avec l'OCAM.

I.3. L'ÉCHANGE D'INFORMATIONS SUR UN COLLABORATEUR ENTRE LES SERVICES DE RENSEIGNEMENT ET UN EMPLOYEUR PRIVÉ OU PUBLIC

En août 2019, le Comité permanent R a reçu une plainte d'une personne qui travaillait pour une institution publique. L'intéressé se plaignait que son employeur avait transmis et demandé des informations le concernant à un service de renseignement, et sur cette base, entendait entreprendre des démarches disciplinaires.

Afin de traiter cette plainte, le Comité a ouvert une enquête visant à déterminer les cas et les conditions dans lesquels une instance privée ou publique peut adresser une demande à l'un des deux services de renseignement sur un collaborateur (ou un candidat à un emploi) ainsi que les cas dans lesquels le service de renseignement concerné peut ou doit y répondre et, le cas échéant, à quelles exigences cette réponse doit satisfaire.[13]

I.3.1. LE CADRE GÉNÉRAL

Qu'un service de renseignement fournisse des informations sur un collaborateur (ou un candidat à un emploi) d'initiative ou à la demande d'un employeur constitue dans les deux cas une ingérence dans la vie privée et dans le droit à la protection

[13] Un avis juridique externe portant sur le respect du droit à la vie privée des travailleurs dans le cadre d'échanges éventuels entre des employeurs et les services de renseignement a été sollicité le 14 avril 2020.

des données à caractère personnel, et ce même s'il s'agit d'une relation de travail. Une telle ingérence n'est permise que s'il existe une base légale claire, si l'ingérence poursuit un objectif légitime et si elle est proportionnée (article 8 de la Convention européenne des droits de l'homme (CEDH), Convention 108 et 108+ et article 22 de la Constitution).

Dans ce cadre, il convient également de mentionner l'article 2 § 1er, alinéa 2, de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) qui dispose que les services de renseignement *'[d]ans l'exercice de leurs missions (…) veillent au respect et contribuent à la protection des droits et libertés individuels, ainsi qu'au développement démocratique de la société'*.

Aucune disposition de la L.R&S n'interdit qu'une instance privée ou publique adresse une demande à l'un des services de renseignement belges. Si un employeur s'adresse à un service de renseignement, il y a une ingérence dans la vie privée que seule une base légale claire rend possible. La L.R&S le permet dans la mesure où l'employeur croit raisonnablement que les informations qu'il communique peuvent être utiles pour l'exécution des missions du service de renseignement concerné (article 14 L.R&S pour les acteurs publics ; article 16 L.R&S pour les acteurs privés).

En ce qui concerne la réponse éventuelle à apporter par le service de renseignement interrogé, le législateur belge n'a prévu que deux cas dans lesquels un employeur (à son initiative ou à l'initiative du service de renseignement) peut obtenir directement ou indirectement des informations sur un collaborateur (ou un candidat à un emploi) : en cas de screening de sécurité ou en cas de menace. Même la simple question de savoir si un collaborateur (ou un candidat à un emploi) est 'connu' ou non d'un des deux services de renseignement belges, doit pouvoir être associée à l'un de ces deux cas de figure.

I.3.2. L'EMPLOYEUR SOUHAITE UN SCREENING DE SÉCURITÉ

I.3.2.1. La base légale pour les screenings de sécurité

Les screenings de sécurité font référence aux situations dans lesquelles un employeur, indépendamment d'un élément antérieur, souhaite que toutes les personnes qui ont besoin d'une autorisation ou d'un permis donné(e) soient soumises à un screening.[14] Un employeur privé ou public peut recourir à cette option dans les conditions prévues par la Loi du 11 décembre 1998 relative à la classification, aux

[14] Les exemples les plus classiques sont ceux d'une habilitation de sécurité en vue d'avoir accès à des informations classifiées, l'attestation de sécurité pour un accès à un lieu ou à un événement déterminé, ou encore un avis de sécurité qui peut être demandé pour des dizaines d'autorisations différentes.

habilitations, attestations et avis de sécurité (L.C&HS). En principe, l'employeur ne recevra que le résultat du screening.[15]

Dans certains cas (par ex. une habilitation de sécurité), le collaborateur est soumis à une forme de 'screening permanent'. En d'autres termes, pendant toute la durée de son habilitation, il devra répondre aux exigences pour disposer de cette habilitation. Si, à un moment donné, un employeur doute de cette condition, il peut consulter son officier de sécurité, qui, à son tour, peut saisir l'autorité de sécurité et/ou le service de renseignement ayant effectué l'enquête. Mais rien n'empêche l'employeur de prendre contact directement avec un service de renseignement s'il estime disposer d'informations utiles pour l'exercice de ses missions (articles 14 ou 16 L.R&S).

Il importe donc de souligner que le cadre légal détermine clairement quelles données à caractère personnel peuvent être transmises, sous quelle forme (par ex. un rapport d'enquête) et à quel destinataire (généralement une autorité de sécurité).

I.3.2.2. Article 19, alinéa 1er, première partie de la phrase L.R&S[16]

Le Comité a rappelé que l'article 19 L.R&S ne constitue pas une base pour la transmission systématique d'informations aux employeurs qui en font la demande dans le cadre des autorisations ou des permis qu'ils doivent accorder.

---

15 C'est l'officier de sécurité – personne désignée au sein d'une instance privée ou publique chargée de faire respecter les règles en matière de classification et personne de contact entre l'instance, l'intéressé et l'autorité de sécurité compétente – qui sera informé des éléments concrets du dossier. Mais cet officier de sécurité sera soumis à un secret professionnel spécifique et sanctionné pénalement (articles 23 et 24 de la Loi Classification) l'empêchant de communiquer tels quels à l'employeur les éléments dont il dispose.

16 Le premier paragraphe complet de l'article 19 L.R&S se lit comme suit: '*Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une [menace] visée aux articles 7 et 11.*'

I.3.3. L'EMPLOYEUR FAIT L'OBJET D'UNE MENACE (PRÉSUMÉE)

I.3.3.1. Article 19, alinéa 1er, dernière partie de la phrase L.R&S

L'article 19 L.R&S s'énonce comme suit : *'Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa (…) qu'aux instances et personnes qui font l'objet d'une [menace] visée aux articles 7 et 11.'*[17]

Cet article constitue une base légale claire pour un service de renseignement aux fins de communication de données (à caractère personnel) à des personnes ou à des instances publiques ou privées[18], et donc, le cas échéant, également à un employeur dont le collaborateur représente une des menaces que doivent suivre la Sûreté de l'État (VSSE) ou le Service Général du Renseignement et de la Sécurité (SGRS) en vertu de la loi.

Cette disposition constitue aussi, en combinaison avec l'article 14 ou 16 L.R&S, la base légale pour un employeur public ou privé inquiet qui interroge un service de renseignement sur son collaborateur parce qu'il estime qu'il représente une menace (potentielle) au sens de la L.R&S.[19] Ces articles sont également la base juridique permettant de communiquer, en réponse à cette question, des éléments concrets sur le collaborateur qui peuvent rendre la menace (présumée) plausible.[20]

I.3.3.2. Une élaboration plus poussée de cette réglementation dans une directive ?

Si la dernière partie de phrase de l'article 19, alinéa 1er L.R&S offre une base juridique suffisamment claire pour la communication d'informations à des

---

17 Le Comité s'est déjà penché sur l'application de la dernière partie de la phrase de l'article 19, alinéa 1er L.R&S dans le cadre de deux précédentes enquêtes : COMITÉ PERMANENT R, *Rapport d'activités 2015*, 41 et suiv. ('II.9. Plainte relative à la transmission d'informations à caractère personnel à un tiers par un agent de renseignement') ; COMITÉ PERMANENT R, *Rapport d'activités 2012*, 14 et suiv. ('II.2. Le suivi par certains services de renseignement étrangers de leur diaspora en Belgique').

18 La loi ne fait référence qu'à des 'instances et personnes'. Il n'y a aucune raison de croire que cette réglementation, hormis la première partie de phrase de l'article 19, alinéa 1er L.R&S, serait limitée aux personnes (morales) publiques.

19 Le fait que le cadre légal permette à un employeur d'un service public de communiquer des informations ou de poser des questions concernant l'un des membres de son personnel aux services de renseignement ne signifie pas que les services de renseignement peuvent ou doivent répondre à la question posée. Le fait que le service de renseignement ne peut (ou ne veut pas) répondre à une question ne rend pas illégal ou fautif le fait d'avoir posé la question.

20 Cette communication/question peut naturellement donner lieu, pour un service de renseignement, à l'ouverture d'une enquête de renseignement. D'un point de vue juridique, l'ouverture ou non d'une telle enquête, plus ou moins approfondie, est distincte de la question de savoir si et ce qu'un service de renseignement peut communiquer à un employeur. Il n'est évidemment pas légitime d'initier une enquête (par définition attentatoire à la vie privée) en l'absence de tout élément indiquant une menace potentielle ou concrète contre les intérêts fondamentaux de l'État.

instances publiques et privées, il existe une obligation de préciser les modalités de cette communication.

Conformément à l'article 20 § 3 L.R&S, le Conseil national de sécurité (CNS) doit définir, dans une directive, les conditions dans lesquelles des renseignements peuvent être communiqués à des instances ou à des personnes privées ou publiques.

Pour autant que le Comité ait pu le constater, cette obligation n'avait pas encore été remplie en ce qui concerne la situation des personnes et des instances qui font l'objet d'une menace.[21] Au terme de l'enquête, le Comité a souligné encore une fois l'importance pour le CNS d'émettre une telle directive offrant des points d'appui aux services de renseignement dans cette matière délicate, où la (non-) communication des informations peut avoir de graves répercussions sur l'intérêt général et sur les intérêts privés.

L'importance d'une telle directive a semblé d'autant plus grande aux yeux du Comité qu'il a pu constater qu'aucune réglementation n'avait été élaborée à cet égard au niveau des services de renseignement. En ce qui concerne la VSSE, il peut néanmoins être fait référence à deux directives. Il y a tout d'abord l'instruction du 10 octobre 2016 classifiée 'CONFIDENTIEL' qui traite de la manière dont le service doit réagir en cas de demande d'une autorité publique de vérifications concernant une personne déterminée. Le Comité a cependant pu constater que cette directive ne précise pas sur la base de quelle législation certaines réponses doivent être apportées et qu'elle ne semble pas s'appliquer à la situation prévue dans la dernière partie de phrase de l'article 19, alinéa 1er L.R&S. Du moins, elle ne règle pas les relations avec les acteurs privés. La légalité de certains passages de cette directive, qui semblent contraires à la réglementation sur les screenings de sécurité, pose par ailleurs question. La VSSE a également établi en 2018 une directive classifiée 'CONFIDENTIEL' sur les actions disruptives ou les entraves.[22] Si la communication d'informations à une personne ou à une instance faisant l'objet d'une menace peut parfaitement entrer dans cette définition, aucune référence n'est faite dans cette directive à l'article 19 L.R&S, ni à aucune autre disposition légale.

I.3.3.3. Les limites posées par la Loi organique des services de renseignement et de sécurité

Dans quels cas et dans quelles limites un service de renseignement peut-il actuellement faire usage de la possibilité d'informer un tiers (public ou privé) des informations dont il dispose ?

---

21 Dans le cadre d'une enquête portant sur la lutte contre le terrorisme et l'extrémisme, le Comité avait déjà insisté sur la nécessité d'une telle directive (COMITÉ PERMANENT R, *Rapport d'activités 2012*, 92).

22 Il s'agit d'entraver les menaces à un point tel qu'elles ne se produisent plus ou que leur nuisibilité s'en trouve considérablement réduite.

En ce qui concerne la VSSE, les menaces visées à l'article 19 L.R&S sont toutes les activités d'espionnage, d'ingérence, de terrorisme, d'extrémisme, de prolifération, ainsi que toutes activités menées par des organisations sectaires nuisibles ou des organisations criminelles susceptibles de mettre en péril la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'État, la sauvegarde du potentiel scientifique ou économique, tel que défini par le Conseil national de sécurité, ou tout autre intérêt fondamental du pays (article 7 L.R&S). Il doit non seulement y avoir une activité bien définie dans le chef du collaborateur (par ex. l'extrémisme), mais celle-ci doit également représenter un danger pour un ou plusieurs intérêts fondamentaux de l'État. Dans le contexte de l'article 19 L.R&S, cette instance privée ou publique doit, en outre, faire l'objet d'une menace. Un employeur ne peut donc pas être informé, par exemple des activités extrémistes de son collaborateur, s'il ne fait nullement l'objet d'une menace.

Par ailleurs, l'article 19 L.R&S ne peut être appliqué que lorsque les intérêts fondamentaux de l'État sont en jeu, et donc pas s'il s'agit uniquement de porter atteinte à l'image d'une entreprise privée (sauf si cela signifie, par exemple, une perte de confiance dans certaines instances), d'une mauvaise ambiance de travail ou d'une perte financière (sauf si ces intérêts financiers dépassent les intérêts individuels de l'entreprise et peuvent être considérés comme fondamentaux pour le pays).

Les menaces qui peuvent amener le SGRS à avertir des instances ou personnes privées ou publiques figurent à l'article 11 L.R&S. Il s'agit, par exemple, de toute activité qui représente une menace pour l'intégrité du territoire national ou la population, les plans de défense militaires, le potentiel scientifique et économique dans les secteurs économiques et industriels liés à la défense, l'accomplissement des missions des Forces armées et/ou la sécurité militaire du personnel relevant du ministre de la Défense.

Étant donné que la communication de données sur la base de la dernière partie de phrase de l'article 19, alinéa 1er L.R&S a une finalité clairement définie (sauvegarde des intérêts fondamentaux de l'État contre certaines activités dont l'instance ou la personne concernée fait l'objet), cette communication doit également se limiter aux informations qui contribuent au suivi ou, si nécessaire, à la neutralisation de la menace.

La première obligation d'un service de renseignement qui se voit confronté à une demande d'informations est par conséquent de vérifier de quel problème, de quel incident, de quelle menace il pourrait s'agir. Dans ce cadre, le service de renseignement pourrait interroger ses banques de données.[23] Il apparaît aussi évident que le service de renseignement prenne contact avec l'employeur afin de bien contextualiser la demande. À cet effet, il conviendra de déterminer notamment

[23] C'est également ce que prescrit la directive de la VSSE du 10 octobre 2016 ('CONFIDENTIEL') dans le cadre d'une demande adressée par une autorité publique en vue de faire procéder à des vérifications sur une personne.

pourquoi l'employeur veut savoir si son collaborateur est connu des services de renseignement, quel est le problème et la menace, s'il y a eu un incident de sécurité ou autre, une urgence, etc.

Si ces données ne sont pas concluantes dans un sens ou dans l'autre, une enquête plus approfondie du service peut être indiquée. L'amplitude de cette dernière ne peut être déterminée *in abstracto*. Elle dépendra de la nature de la menace et des informations qui apparaîtront au cours de celle-ci. Dans le cadre d'une telle enquête, le service devra en tout cas tenir compte des principes de proportionnalité et de subsidiarité.

Les réponses à ces questions et les résultats de l'enquête complémentaire doivent permettre au service de renseignement d'évaluer s'il est compétent en la matière et, le cas échéant, s'il peut appliquer l'article 19 L.R&S. Ces réponses doivent également permettre au service de renseignement de déterminer ce qu'il peut ou non communiquer à l'employeur compte tenu de la menace.

I.3.3.4. Qu'est ce qui peut ou doit être communiqué ?

Dans ce qui suit, on part du principe qu'il existe effectivement une menace. La question se pose alors de ce qui peut être communiqué de quelle manière.[24]

I.3.3.4.1. Les principes de proportionnalité et de subsidiarité

Compte tenu des exigences de proportionnalité et de subsidiarité, la première question doit être de savoir si l'employeur peut être informé. Si la menace est très vague et peu grave, ou si le service peut lui-même suivre l'évaluation de la menace ou encore si la menace peut être contrée d'une autre manière (par ex. en s'adressant au collaborateur de sorte qu'il soit conscient d'être suivi), il se peut que la communication de données à caractère personnel à un employeur soit disproportionnée et non subsidiaire.

Si cela ne suffit pas et que la menace est suffisamment grave, la possibilité se présente alors d'en informer l'employeur. Ici aussi, il faut tenir compte de la quantité et du type d'informations qui sont données. Une fois encore, la règle est que, compte tenu de la nature et de la gravité de la menace et de la nécessité et

[24] Tout d'abord, l'hypothèse brièvement évoquée est celle du service de renseignement qui n'identifie absolument aucune menace dans le chef du collaborateur au sens de la L.R&S (éventuellement après avoir questionné une première fois ledit collaborateur ou après une enquête plus approfondie). À ce moment-là, l'employeur ne fait, par définition, pas l'objet d'une menace et *sensu stricto* l'article 19 L.R&S ne peut être appliqué. Le Comité estime cependant que dans ces cas, le service de renseignement doit avoir la possibilité d'informer l'employeur qu'il n'y a pas de menace au sens de la L.R&S (ce qui ne signifie évidemment pas que l'employeur ne peut pas faire l'objet d'une autre menace). Le Comité s'est déjà prononcé en ce sens dans une enquête précédente (COMITÉ PERMANENT R, *Rapport d'activités 2015*, 41 et suiv. ('II.9. Plainte relative à la transmission d'informations à caractère personnel à un tiers par un agent de renseignement')).

des options disponibles pour la contrer, l'objectif doit être une ingérence minimale dans la vie privée.

Cependant, si la menace est si grave qu'elle ne peut être contrée que par l'intervention de l'employeur, davantage d'informations et des informations plus concrètes peuvent être communiquées. Ces informations peuvent, par exemple, servir à motiver une décision administrative ou privée (une sanction disciplinaire, une mutation, un licenciement, etc.). De toute évidence, l'objectif ultime du service de renseignement doit être dans ce cas-ci de neutraliser ou d'atténuer une menace.

Dans le prolongement de la question de la communication proportionnée des informations, un service de renseignement peut-il, dans le cadre de sa communication, lui-même proposer une solution à l'instance publique ou privée qui est menacée, voire participer à la prise de décision de l'instance ou de la personne menacée sur la manière de traiter cette menace (par ex. suggérer un licenciement) ? Le Comité a estimé que ceci n'est pas illégal dans la mesure où la solution qui est suggérée est elle-même légale et proportionnée.

Enfin, la question s'est posée de savoir si l'article 19 L.R&S prévoit une obligation de répondre à une question ou de fournir des informations d'initiative. La disposition prévoit que les services de renseignement et de sécurité 'ne communiquent' leurs renseignements 'qu'aux' instances et personnes qui font l'objet d'une menace. Même si la disposition dans ce domaine n'est pas très claire, le Comité a estimé qu'un service de renseignement est tenu de communiquer des données s'il s'agit du seul moyen d'empêcher la concrétisation d'une menace grave contre les intérêts fondamentaux de l'État. Dans les autres cas, le service définit la meilleure stratégie en toute autonomie, en fonction de la menace. Le Comité a recommandé de pallier ce manque de clarté, soit via une initiative législative, soit via une clarification en la matière dans la directive que doit émettre le CNS.

Dans la foulée, le Comité a suggéré d'examiner s'il serait utile de prévoir une notification obligatoire à l'employeur pour chaque collaborateur (ou candidat à un emploi) figurant dans la Banque de données commune *Terrorist Fighters* ou Prédicateurs de haine.

I.3.3.4.2. Autres points d'attention : précaution, classification, communication écrite

Dans un contexte de renseignement, il y a peu de certitudes, et ce fait doit influencer la décision d'informer ou non un employeur ainsi que la manière de le faire. Pour pouvoir être considérée comme légale, la communication d'informations doit être

suffisamment étayée par des informations fiables. Elle doit également être formulée avec précaution.[25]

Par ailleurs, toutes les instances privées et publiques ne disposent pas d'une habilitation de sécurité, ce qui signifie que les informations classifiées devront être déclassifiées. Ceci est d'autant plus vrai si les informations doivent servir à étayer une décision de l'employeur.

Enfin, l'article 19 L.R&S ne précise pas comment informer une autorité qui est menacée. Le Comité a estimé que, pour des raisons de sécurité juridique, cette notification devrait se faire par écrit, sauf en cas d'urgence, afin d'éviter les discussions *a posteriori* et de permettre un contrôle parlementaire, et même judiciaire.

I.3.4. CONCLUSIONS

Des règles strictes s'appliquent, à raison, à la communication d'informations par les services de renseignement à un employeur privé ou public. En effet, la communication d'informations peut avoir des conséquences non négligeables pour les personnes concernées. À tout le moins, cela signifie une atteinte à la vie privée et, dans les cas extrêmes, cela peut constituer la base de mesures intrusives pouvant affecter la situation juridique des intéressés.

Si la VSSE et le SGRS fournissent des informations à un employeur public ou privé, que ce soit d'initiative ou sur demande (en ce compris le fait de simplement informer que la personne est 'connue' ou non), ils doivent respecter toutes les exigences légales :

1. Une base légale spécifique doit exister ;
2. Il faut faire preuve de vigilance dans la production interne des données à fournir et dans leur communication au destinataire ;
3. La communication doit répondre aux exigences de nécessité ;
4. La communication doit être proportionnée.

En ce qui concerne la base légale, le Comité a souligné qu'en dehors des deux situations évoquées (c.-à-d. l'employeur veut un screening de sécurité ou l'employeur fait l'objet d'une menace), il n'est pas permis de fournir des informations sur un collaborateur à un employeur public ou privé. Du point de vue de l'agent de

[25] Par exemple, aucune image sans nuance ne peut être donnée des renseignements sous-jacents, ou un élément particulier ne peut être présenté comme étant une 'vision de' ou une 'impression de'. En ce sens, les informations fournies doivent également être 'justes' en offrant une image objective de la façon dont le service de renseignement perçoit la menace et le rôle de la personne concernée, sans être 'manipulatrices' au sens où elles viseraient à orienter les décisions des employeurs privés ou publics.

renseignement, ce genre de communication peut même être punissable en fonction de la situation concrète.

Le Comité a souligné également que rien n'empêche un employeur du secteur public ou privé de communiquer des informations ou d'interroger un service de renseignement belge concernant une éventuelle menace, au sens de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S), dont l'un des collaborateurs serait l''auteur'.

Au terme de l'enquête, le Comité invitait cependant les acteurs des secteurs publics et privés à examiner si certaines menaces potentielles ne peuvent pas être évitées en recourant, pour certaines fonctions, autorisations ou permis, au système de screening de sécurité prévu dans la Loi Classification, en ayant un recours judicieux à ce système.

Le Comité estimait que la VSSE et le SGRS, dans les six mois suivant la conclusion de cette étude, devaient rédiger une directive visant à mettre en œuvre la dernière partie de phrase de l'article 19, alinéa 1er L.R&S et l'adresser aux ministres de la Justice et de la Défense pour soumission au Conseil national de sécurité invité à l'approuver.

I.4. DYSFONCTIONNEMENTS GRAVES EN MATIÈRE DE SÉCURITÉ NATIONALE

Début juillet 2020, le président du Comité permanent R adressait un courrier classifié au ministre des Affaires étrangères et de la Défense (de l'époque), compétent notamment de l'Autorité nationale de sécurité (ANS) et du SGRS. En sa qualité de président de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité[26], de graves dysfonctionnements en matière de sécurité nationale avaient été constatés.

Était en cause un dossier de renouvellement en janvier 2020 d'un avis de sécurité par une travailleuse qui avait reçu un avis positif en 2015. Ce dernier lui donnait le droit d'accéder aux zones de l'aéroport de Bruxelles National dont les accès sont limités pour des raisons de sécurité. Il ressortait cependant d'un rapport classifié que le partenaire de l'intéressée était un des co-auteurs présumés des attentats de Paris et Bruxelles, et qu'elle entretenait avec lui des contacts réguliers lors de visites en prison dans une pièce sans surveillance.

[26] L'organe de recours est une juridiction administrative compétente pour connaitre des recours relatifs aux habilitations, attestations et avis de sécurité dans le cadre de la Loi du 11 décembre 1998. Le président de l'Organe de recours est également le président du Comité permanent R. À ce propos, voir 'Chapitre IX. L'organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité'.

Nonobstant le risque sécuritaire indéniable, la décision de retrait de l'avis ou de l'habilitation de l'intéressée ne fût prise qu'à l'introduction de la demande de renouvellement.[27]

Le Comité permanent R a interpellé le gouvernement soulignant que cela mettait en évidence le 'dysfonctionnement' des administrations et services publics dans le domaine de la sécurité, le travail en silo empêchant de garantir la sécurité du citoyen. Le Comité permanent R a souligné la récurrence de ce problème qui avait déjà été mis en exergue par les travaux de la Commission parlementaire 'Attentats terroristes' du 22 mars 2016.[28]

S'en est suivi, entre juillet 2020 et février 2021, un échange de lettres entre le Comité permanent R, le ministre des Affaires étrangères et de la Défense (de l'époque), le président de l'ANS et le président du Collège des procureurs généraux. Il a notamment été demandé qu'un groupe de travail soit mis en place pour analyser les dysfonctionnements identifiés.

Le Comité permanent R a dû constater que peu d'attention était accordée aux problèmes de sécurité nationale qui avaient été soulevés.[29] Ayant atteint les limites de ses prérogatives, le Comité a confié la situation à la Chambre des représentants pour suite utile. Les remarques du Comité permanent R auraient été intégrées dans les travaux des différents groupes de travail mis en place au sein de l'ANS se penchant notamment sur une réforme structurelle de l'ANS.

I.5. LE SUIVI DES ORGANISATIONS SECTAIRES NUISIBLES ET DES ORGANISATIONS CRIMINELLES PAR LA SÛRETÉ DE L'ÉTAT

À la demande de la Commission de suivi, le Comité permanent R a ouvert une enquête visant à analyser la manière dont la VSSE exécutait deux de ses missions

---

27 L'enquête de contrôle sur la manière dont les services de renseignement réalisent les screenings de sécurité a également accordé une attention particulière à cette problématique. Voir COMITÉ PERMANENT R, *Rapport d'activités 2019*, 2-14 ('I.1. La réalisation de screenings de sécurité par les services de renseignement').

28 CHAMBRE DES REPRÉSENTANTS DE BELGIQUE, *Commission d'enquête Attentats terroristes 22 mars 2016. Résumé des travaux et recommmandations*, 2018.

29 Le sujet a fait l'objet de questions parlementaires (cf. Question de C. Thibaut à la ministre des Affaires étrangères sur 'l'absence de réponses de l'ANS au Comité R en matière d'habilitations de sécurité' (*Q.R.*, Chambre 2020-2021, 15 juillet 2021, n°59, p.108, Q. n°601) et d'articles de presse (par ex. L. BOVÉ, *De Tijd*, 6 mai 2021 ('Kamer slaat alarm over veiligheidsscreenings').

légales, à savoir le suivi des menaces que constituent les organisations sectaires nuisibles[30] et les organisations criminelles.[31]

I.5.1. CONTEXTUALISATION

I.5.1.1. Les organisations sectaires nuisibles

Longtemps, les autorités belges ont traité les mouvements réputés sectaires avec une réserve toute particulière. Cette attitude était dictée par la difficulté à prendre position dans un domaine touchant aux libertés fondamentales de religion, de pensée, d'expression et d'association.

Au cours des années 1980, plusieurs événements tragiques et très médiatisés ont attiré l'attention de la population et des autorités sur ce phénomène, ce qui a conduit à plusieurs initiatives en Belgique dans les années 1990. C'est ainsi qu'a été mise sur pied, en 1996, une commission d'enquête parlementaire 'sectes'.[32] Le Centre d'information et d'avis sur les organisations sectaires nuisibles (CIAOSN) ainsi que la cellule administrative de coordination (CAC) ont été institués par la Loi du 2 juin 1998.[33] Le secrétariat de la CAC a été attribué à la Sûreté de l'État.[34]

---

30 Le Comité entend par « secte », « organisation sectaire nuisible » ou « groupement sectaire nuisible », tout groupement à vocation philosophique ou religieuse, ou se prétendant tel, considéré comme nuisible et susceptible, à ce titre, de faire l'objet d'un intérêt quelconque de la part de la VSSE.

31 Le Comité avait déjà, dans le passé, pu se pencher sur plusieurs aspects de cette problématique.
Concernant les organisations sectaires : COMITÉ PERMANENT R, *Rapport d'activités 1996*, 86-96 ("Chapitre II. Enquête sur l'efficacité des services de renseignements relative à l'activité des sectes en Belgique") ; *Rapport d'activités 2006*, 60-61 ("II.6.2. Les organisations sectaires nuisibles et la compétence de la Sûreté de l'État") ; *Rapport d'activités 2007*, 40 ("II.10.9. Organisations sectaires nuisibles") ; *Rapport d'activités 2010*, 13-23 ("II.2. Le suivi des organisations sectaires nuisibles") ; *Rapport d'activités 2014*, 52-55 ("II.5. Une plainte de l'église de Scientologie contre la Sûreté de l'État ")
Concernant les organisations criminelles : COMITÉ PERMANENT R, *Rapport d'activités 2002*, 19-20 (« Chapitre II.2.6 Enquête de contrôle sur les renseignements dont dispose la Sûreté de l'État à propos d'une affaire de fraude aux visas évoquée au Sénat » ; *Rapport d'activités 2004*, 12-18 (IV.2.2 « Enquête sur la manière dont les services de renseignement belges fonctionnent et collaborent dans le cadre de leur nouvelle mission légale concernant les menaces des organisations criminelles ».

32 *Doc. parl.*, Chambre, 1995-1996, n° 313/008.

33 La Loi du 2 juin 1998 portant création d'un Centre d'information et d'avis sur les organisations sectaires nuisibles et d'une Cellule administrative de coordination de la lutte contre les organisations sectaires nuisibles (*M.B.* 25 novembre 1998). Celle-ci prévoit une collaboration active entre le CIAOSN, la CAC et les autres services publics impliqués dans la lutte contre les sectes nuisibles dont le Parquet fédéral, les Parquets généraux, les Parquets, la Police, la Sûreté de l'État et les autorités locales.

34 Arrêté royal du 8 novembre 1998 fixant la composition, le fonctionnement et l'organisation de la Cellule administrative de coordination de la lutte contre les organisations sectaires nuisibles (*M.B.* 9 décembre 1998).

I.5.1.2. Les organisations criminelles

En 2019, la Police Judiciaire Fédérale a réalisé une étude sur les organisations criminelles dans le cadre de laquelle plus de 600 organisations criminelles, associations de malfaiteurs ou groupes d'auteurs ont été renseignés en Belgique.[35]

Dans son rapport de 2020[36], la Cellule de Traitement des Informations Financières (CTIF) mentionne à son tour que 31.605 déclarations lui ont été adressées en 2020. Elle ajoute que 1.228 nouveaux dossiers ont été transmis en 2020 aux autorités judiciaires et que des informations issues de 2.765 déclarations de soupçon ont été utilisées dans une transmission aux Parquets et Parquet fédéral pour un montant total de 1.885,31 millions d'euros. Le rapport précise également que « *2020 a été marquée par un nombre important de dossiers transmis par la CTIF en lien avec la criminalité organisée* ».[37]

I.5.2. LA COMPÉTENCE MATÉRIELLE

La mission de la VSSE en matière de suivi des sectes nuisibles et des organisations criminelles se situe dans le cadre de sa mission de renseignement. Conformément à l'article 7, 1° L.R&S, la VSSE a pour mission *'de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'État et les relations internationales, le potentiel scientifique ou économique défini par le Conseil national de sécurité, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité'*.

Le législateur a choisi de dresser une liste limitative des menaces pour la sécurité qui relèvent du domaine de compétence de la VSSE (c'est-à-dire le terrorisme, l'extrémisme, l'espionnage, l'ingérence, la prolifération, les organisations sectaires nuisibles et les organisations criminelles).

Les *'organisations sectaires nuisibles'* sont décrites comme étant *'tout groupement à vocation philosophique ou religieuse, ou se prétendant tel, qui, dans son organisation ou sa pratique, se livre à des activités illégales dommageables, nuit aux individus ou à la société ou porte atteinte à la dignité humaine'* (art. 8, 1°, alinéa 2, L.R&S).

Le législateur a, en outre, désigné les *'organisations criminelles'* comme étant une menace pour la sécurité nationale qui doit relever de la sphère d'intérêt de la VSSE. Cette notion est décrite comme suit dans la Loi organique des services de renseignement et de sécurité : *'toute association structurée de plus de deux*

---

35 Police fédérale belge, 'Diagnostic- Vers une première approche des organisations criminelles', Avril 2020, 4. La PJF souligne que 'la problématique du terrorisme ou de son financement y est citée 20 fois'.

36 https://www.ctif-cfi.be/images/documents/French/Rapports_annuels/ra2020.pdf, 10.

37 https://www.ctif-cfi.be/images/documents/French/Rapports_annuels/ra2020.pdf, 22.

personnes, établie dans le temps, en vue de commettre de façon concertée des crimes et délits, pour obtenir, directement ou indirectement, des avantages patrimoniaux, en utilisant l'intimidation, la menace, la violence, des manœuvres frauduleuses ou la corruption ou en recourant à des structures commerciales ou autres pour dissimuler ou faciliter la réalisation des infractions.' (art. 8, 1°, alinéa 2, f) L.R&S).[38]

La VSSE n'est compétente que pour le suivi des organisations criminelles '*qui se rapportent intrinsèquement aux activités visées à l'article 8, 1°, a) à e) et g)*' – c'est-à-dire les activités de terrorisme, d'extrémisme, d'espionnage, d'ingérence, de prolifération et de sectes nuisibles – *'ou qui peuvent avoir des conséquences déstabilisantes sur le plan politique ou socio-économique*'.

Toutes les organisations sectaires nuisibles et toutes les organisations criminelles ne font donc pas partie de la sphère d'intérêt légale de la VSSE. La Loi organique des services de renseignement et de sécurité prévoit, en outre, que ces organisations ne relèvent de la compétence de la VSSE que si leurs activités sont susceptibles de représenter une menace pour la sécurité intérieure ou extérieure de l'État et/ou pour le potentiel économique ou scientifique du pays.

Le Comité relevait en 2015 l'exception que constituait la Belgique en attribuant à son service de renseignement civil la mission de suivi des organisations sectaires nuisibles : « *aucun autre service de renseignement étranger n'a pour mission officielle de surveiller les sectes nuisibles. Cette mission spécifique de la Sûreté de l'État belge constitue donc une exception dans le monde des services de renseignement.*[39] *La plupart des pays démocratiques refusent même d'impliquer ces services dans la surveillance des mouvements religieux. Parce que cette mesure pourrait être considérée comme une atteinte à la liberté religieuse* ».

I.5.3. LA COMPÉTENCE PROCÉDURALE

La compétence procédurale dans le cadre de la mission de renseignement est déterminée en premier lieu par les activités énumérées à l'article 7, 1° L.R&S : *'(de) rechercher, (d') analyser et (de) traiter le renseignement*'. Il en ressort que la VSSE est chargée de lutter contre les sectes nuisibles et les organisations criminelles en recueillant des informations et en analysant les renseignements, puis en transmettant à d'autres instances (par ex. les autorités policières ou judiciaires) les renseignements obtenus (c'est-à-dire les informations enrichies). Ces instances prendront finalement les contre-mesures qui s'imposent pour protéger la sécurité nationale.

---

38 Le législateur a voulu établir une distinction entre une organisation criminelle comme menace pour la sécurité nationale et une organisation criminelle comme infraction pénale (art. 324*bis* CP).

39 A laquelle la VSSE ajoute (14 avril 2021): "*et le service, au surplus, se trouve privée d'échanges fructueux en la matière avec ses correspondents étrangers*".

Pour réaliser ces missions, la VSSE y affectait, au pic de son activité en ces matières, le personnel suivant :

– *Organisations sectaires nuisibles (1999-2000)* : 6 personnes en 'Section Analyse' (dont 3 niveaux A) et 9 personnes en 'Section Opérationnelle' ;
– *Organisations criminelles* (*années 2000*) : 2 personnes en 'Section Analyse' et 2 personnes en 'Section Opérationnelle'.

I.5.4. LES PRIORITÉS POLITIQUES

Si l'article 7, 1° L.R&S établit une obligation légale d'agir dans le chef de la VSSE, cela ne signifie pas pour autant qu'aucune priorité ne peut être fixée dans le cadre de ses activités. En effet, le service ne dispose pas (et ne pourrait jamais disposer) de capacités et de ressources suffisantes pour détecter, surveiller et contrôler toutes les menaces pour la sécurité nationale relevant de sa compétence. La hiérarchisation des priorités est donc une nécessité, voire une obligation.

Cette lecture est confirmée dans diverses dispositions légales et réglementaires. Tout d'abord, l'article 4 L.R&S stipule que la VSSE accomplit ses missions à l'intervention du ministre de la Justice, mais *'conformément aux directives du Conseil national de sécurité'*.

La mission du CNS est définie à l'article 3 de l'Arrêté royal du 22 décembre 2020 'portant création du Conseil national de sécurité, du Comité stratégique du renseignement et de la sécurité et du Comité de coordination du renseignement et de la sécurité'. Celui-ci établit que le CNS, *'(e)n tant qu'organe de coordination', 'est chargé de la définition des priorités des services de renseignement et de sécurité'*.

En juillet 2015, ce même Conseil national de sécurité a décidé que la VSSE n'assurerait plus un suivi actif des organisations sectaires nuisibles et des organisations criminelles. Cette décision a été prise sous l'impulsion des ministres de la Justice et de la Défense souhaitant, suite à la vague d'attentats et de tentatives d'attentats en Belgique et à l'étranger, redéfinir la priorité des missions des services de renseignement belges et la réaffectation de leurs moyens en personnel et matériel.

Le 25 août 2015, le ministre de la Justice de l'époque explique que « *De Staatsveiligheid reoganiseert vanaf 1 september haar buitendienst met een ongeziene focus op het radicalisme en het terrorisme* ». Dans ce cadre, la Sûreté de l'État communiquera encore que « *Le plan d'action 2015 de la Sûreté de l'État a été approuvé par le Conseil national de sécurité. Sur la base de ce plan, des décisions ont été prises par la direction de la Sûreté de l'État concernant son organisation* », ajoutant encore « *Conséquence de ce recentrage : les autres menaces telles que les*

sectes et l'espionnage industriel se retrouveront à l'arrière-plan ».[40] En 2020, la VSSE l'a également confirmé en indiquant que le '*suivi actif des organisations sectaires nuisibles a été mis en suspens, sauf au cas où une menace d'ingérence, d'espionnage, de prolifération, d'extrémisme ou de terrorisme y serait liée*'. Le même constat vaut pour les organisations criminelles.

L'article 2 de l'Arrêté royal du 5 décembre 2006 relatif à l'administration générale et à la cellule d'appui de la Sûreté de l'État dispose que la direction générale de la VSSE (c'est-à-dire l'Administrateur général et l'Administrateur général adjoint) est '*responsable de l'élaboration et de la mise en œuvre d'un plan stratégique quadriennal qui détermine les priorités de la Sûreté de l'État et les stratégies opérationnelles pour mettre en œuvre ces priorités*'. L'article 3 stipule que '*les administrateurs généraux de la VSSE soumettent conjointement chaque année au Ministre de la Justice un plan d'action*' lié à la réalisation des priorités du plan stratégique. Ce plan d'action comprend, entre autres, les objectifs stratégiques et les moyens de les concrétiser. L'analyse de ces plans montre que depuis les attentats de Verviers (janvier 2015), Paris (novembre 2015) et Bruxelles (mars 2016), le terrorisme et l'extrémisme (islamiste, de droite et de gauche), ainsi que l'espionnage, constituent les trois fers de lance de la politique de la VSSE et, en tant que tels, sont considérés comme les menaces les plus importantes. Ni les organisations sectaires nuisibles ni les organisations criminelles ne figurent dans la liste des priorités.

I.5.5. LA MARGE DE MANŒUVRE AUTORISÉE

Lorsqu'ils fixent les priorités politiques, le Conseil national de sécurité et le ministre de la Justice sont soumis à des contraintes juridiques. Les priorités doivent d'abord se situer dans la sphère de compétence définie par le législateur, c'est-à-dire dans le cadre des intérêts à protéger et des menaces pour la sécurité qu'il convient de contrer.

En outre, ni le Conseil national de sécurité, ni le ministre de la Justice, pas plus que la VSSE, ne sont compétents pour décider qu'une menace pour la sécurité, dans son intégralité, pour tous les types d'activités de renseignement et en tout temps, ne doit pas faire l'objet d'un suivi. Une telle mesure équivaut à une suspension par le pouvoir exécutif de l'article 7, 1° *p.o.* article 8, 1° L.R&S. L'établissement de priorités dans le cadre des missions de renseignement de la VSSE consiste à déterminer les questions pour lesquelles le service de renseignement doit constituer activement

[40] Le ministre de la Justice confirmera en 2016 encore ce changement d'orientation dans sa réponse à une question parlementaire et précisera qu'un projet modificatif est en cours de rédaction visant à décharger la Sûreté de l'État du secrétariat de la Cellule administrative de coordination, et à la confier au secrétariat du CIAOSN. (Question de K. JADIN au ministre de l'Intérieur sur la « surveillance des sectes » (*C.R.I.*, Chambre 2016-2017, 9 novembre 2016, COM 529, p.14, Q. n° 14723).

une position d'information. Cela ne signifie en aucun cas que si la VSSE reçoit passivement des informations d'un tiers contenant des indications concrètes (*leads*) d'éventuelles activités problématiques[41], la VSSE n'aurait pas le devoir de procéder à une évaluation approfondie et, si nécessaire, d'enquêter activement.[42]

I.5.6. LA TRADUCTION ORGANISATIONNELLE DES PRIORITÉS POLITIQUES

Il convient par ailleurs de se demander dans quelle mesure cette marge de manœuvre juridiquement limitée impacte la traduction organisationnelle des priorités politiques. En d'autres termes : qu'est-ce qui est et qu'est-ce qui n'est pas possible dans le cadre de la création et de la dissolution de services et de sections ? Et faut-il prévoir une capacité réservée ?

Le ministre de la Justice (*cf*. art. 5, § 3 L.R&S) et, à titre subsidiaire, la direction générale de la VSSE (*cf*. art. 2 A.R. 5 décembre 2006) ont, dans le cadre des règles définies par le législateur et le Roi, la responsabilité de définir la structure organisationnelle de la VSSE.[43]

Dans ce cadre législatif et réglementaire, il est laissé à la discrétion du pouvoir exécutif de créer ou non un service (d'analyse) ou une section (opérationnelle) pour une menace de sécurité particulière. La suppression du service d'analyse Sectes et, auparavant, de la section opérationnelle Sectes au sein de la VSSE, relève donc de l'autonomie des décideurs politiques susmentionnés.

Cependant, la VSSE doit s'organiser de manière à pouvoir remplir son obligation légale d'agir lorsqu'elle reçoit passivement des informations d'un tiers contenant des indications concrètes d'éventuelles activités problématiques de sectes nuisibles ou d'organisations criminelles. Une capacité réservée (par ex., x analystes et x agents de collecte) chargée d'examiner ces informations obtenues passivement et, le cas échéant, de recueillir des informations supplémentaires

---

41 Par ex. d'organisations sectaires nuisibles ou d'organisations criminelles telles que définies par la loi.

42 La VSSE a certes la compétence de procéder à une évaluation d'opportunité dans le cadre de ses enquêtes, mais elle a également l'obligation d'enquêter sur les menaces pour la sécurité énumérées par le législateur. Compte tenu du principe de précaution, l'évaluation de *leads* et la décision subséquente de les poursuivre activement ou non, doivent être prises sur la base de critères objectifs préétablis. Compte tenu du principe de légalité, ces critères ne doivent pas conduire à une situation où une menace pour la sécurité définie légalement ne fait jamais l'objet d'une enquête approfondie dans la pratique.

43 Au niveau gouvernemental, l'Arrêté royal du 5 décembre 2006 (*supra*) stipule que la VSSE est composée d'une direction des opérations, d'une direction de l'analyse et d'une direction d'encadrement. Au niveau législatif, la Loi relative à la classification stipule, par exemple, que la VSSE doit disposer d'un officier de sécurité, tandis que la Loi relative à la protection des données stipule que le service doit disposer d'un délégué à la protection des données.

pourrait ainsi être prévue.[44] Ces agents de la VSSE pourraient encore être chargés d'autres tâches définies par le responsable de la VSSE, mais ils jouraient un rôle de première ligne lorsque des informations problématiques sur les sectes ou les organisations criminelles sont transmises à la VSSE.

I.5.7. BESOIN DE RENFORTS ET D'UN DÉBAT SOCIÉTAL

Au terme de l'enquête, le Comité a pu établir que la priorisation des missions du service était conforme au cadre légal et réglementaire.

Après avoir constaté qu'en 2021 la VSSE n'était à même de suivre qu'une partie assez faible de dossiers ouverts – et qu'il en résultait indéniablement pour cette administration (en manque d'effectifs) l'obligation d'effectuer des choix – le Comité a rappelé les demandes pressantes de la VSSE quant à l'augmentation de ses moyens en personnel, financiers et quant à la détermination exacte de ses missions légales.

Enfin, dans ses conclusions, le Comité posait le constat qu'un débat sociétal plus large (lisez : parlementaire ?[45]) s'imposait sur les missions dévolues au service de renseignement civil dans la Loi organique des services de renseignement et de sécurité de 1998 et l'établissement des priorités qui y sont associées. Et par conséquent, l'attribution de capacités et de ressources suffisantes pour détecter, surveiller et contrôler l'ensemble des menaces pour la sécurité nationale relevant de la compétence de la VSSE devrait faire l'objet d'une discussion approfondie.

---

44 La VSSE précise à cet égard (14 avril 2021): *"La Sûreté de l'État applique déjà la recommandation de constituer une 'capacité réservée', à la fois opérationnelle et d'analyse, mobilisable le cas échéant pour assurer un traitement adéquat des informations reçues relatives aux organisations sectaires nuisibles et aux organisations criminelles, au cas où elles intéresseraient la Sûreté de l'État ou le potential scientifique ou économique de la Belgique*".

45 La VSSE réfléchit dans le même sens (14 april 2021): "*C'est au Parlement, tant dans sa fonction de législation que de controle du pouvoir exécutif, qu'il appartiendra d'apprécier (considérant les moyens humains et matériels limités dont la VSSE dispose et la gravité parfois extrême des nombreuses menaces liées à l'extrémisme, au terrorisme, à l'ingérence, à l'espionnage et à la prolifération auxquelles elle est confrontée in concreto) si il est opportun ou bien d'exiger de la Sûreté de l'État qu'elle assure à nouveau le suivi actif des organisations sectaires nuisibles, ou bien de l'en décharger, ou bien de valider la décision du Conseil national de sécurité du 13 juillet 2015 approuvant la mise en suspens du suivi actif des organisations sectaires nuisibles.*"

I.6. L'ATTENTION DES SERVICES DE RENSEIGNEMENT BELGES POUR UN COLLABORATEUR DU SGRS ET SES LIENS AVEC DES CITOYENS RUSSES[46]

En 2014-2015, la VSSE et le SGRS ont conjointement mené une enquête sur un officier de réserve de la Direction I (Renseignement) (de l'époque) du SGRS.

L'auteur des faits entrait déjà en 2008 dans la ligne de mire de la VSSE suite au signalement d'un partenaire étranger. En 2012, son nom est à nouveau mentionné. L'intéressé est situé comme 'cible périphérique' d'un oligarque russe. Deux ans plus tard, la VSSE prendra connaissance de sa qualité d'officier de réserve au SGRS. Une collaboration est alors lancée avec le SGRS. Les éléments en possession des deux services de renseignement semblent mettre en évidence des faits d'espionnage. En février 2015, le SGRS lui retire son habilitation de sécurité. La décision de retrait est confirmée par l'Organe de recours qui a été saisi de l'affaire. Le dossier est clôturé début juillet 2015 par la VSSE. L'intéressé semblait informé de l'enquête menée sur sa personne.

Sur la base des éléments récoltés par le SGRS et la VSSE et lui ayant été communiqués, le Comité permanent R n'a pas pu conclure en l'existence ou non de faits d'espionnage dans le chef de l'intéressé. Depuis la décision de l'Organe de recours, l'auteur des faits a quitté la Défense.

I.7. LE SCREENING DE SÉCURITÉ DES MILITAIRES ET DES CIVILS À LA DÉFENSE

Chaque année, la VSSE et le SGRS passent au crible plusieurs milliers de personnes qui veulent obtenir l'une ou l'autre licence ou autorisation, ou qui souhaitent exercer une fonction déterminée. Ce faisant, ils entendent vérifier si les intéressés offrent des garanties suffisantes en termes de fiabilité et de sécurité. Précédemment, le Comité a ouvert une enquête de contrôle plus large sur la manière dont les services de renseignement réalisent les screenings de sécurité.[47] [48]

---

[46] Cette brève enquête avait pour but d'informer la Commission de suivi suite à la demande d'information adressée par un membre de ladite Commission au Comité permanent R le 6 juin 2019.

[47] Par screening de sécurité, on entend « *une évaluation imposée par la loi et conforme à celle-ci, effectuée par une autorité administrative sur la base des données (à caractère personnel) dont elle dispose déjà ou qui lui ont été communiquées, par laquelle elle décide si le profil d'une personne (morale) privée présente ou peut présenter un risque d'usage non approprié d'une autorisation déterminée susceptible de mettre en péril certains intérêts fondamentaux (de l'État), de sorte que cette même autorité ou une autre autorité (étrangère) qui en est informée peut décider de l'octroi, du retrait ou de la limitation de cette autorisation.* ».

[48] COMITÉ PERMANENT R, *Rapport d'activités 2019*, 2 et suiv. ('La réalisation des screenings de sécurité par les services de renseignement').

Suite à cette enquête, il a été constaté que certains membres du personnel de la Défense n'ont jamais été soumis à un tel screening de sécurité au moment de leur candidature, de leur recrutement ou au cours de leur carrière, ou seulement une fois. Par conséquent, le Comité permanent R s'est penché sur le screening du personnel militaire et civil de la Défense (I.7.1.), ainsi que sur le screening des étudiants de l'École Royale Militaire (I.7.2.).

I.7.1. LE SCREENING DES MILITAIRES ET DES CIVILS DE LA DÉFENSE

La Loi du 28 février 2007 fixant le statut des militaires et candidats militaires du cadre actif des Forces armées décrit notamment la procédure de recrutement.

Les candidats militaires doivent satisfaire à diverses conditions : ils doivent jouir de leurs droits civils et politiques, et disposer des qualités morales indispensables (artt. 8 et 9). Enfin, ils ne peuvent pas avoir reçu un avis de sécurité négatif après une vérification de sécurité ou avoir refusé celle-ci. Cela signifie que, sauf à considérer que la carrière de l'intéressé impose une modification du niveau de sécurité, un militaire du département de la Défense ne subit qu'un seul *screening* de sécurité durant l'entièreté de sa carrière militaire. Le Comité était d'avis qu'il y avait lieu de se demander si une vérification de sécurité ne devrait pas se répéter périodiquement durant la carrière du personnel militaire.[49]

La situation est différente pour les (candidats) civils auprès de la Défense.[50] La grande majorité du personnel civil, soit 1.100 personnes, est statutaire ; ces fonctionnaires ayant été nommés et ayant prêté serment. Un deuxième groupe de civils est constitué par les contractuels qui sont engagés sur la base d'un contrat de travail, exactement comme dans le secteur privé. Par ailleurs, il y a encore des civils qui ne sont pas considérés comme du personnel de la Défense (p. ex. des chercheurs engagés par le Patrimoine, des professeurs détachés des Communautés à l'École Royale des Sous-Officiers…). Tout recrutement civil, à l'exception des contrats Rosetta[51], passe obligatoirement par le SELOR.

À de rares exceptions près[52], les civils du Département de la Défense ne font l'objet d'aucune vérification de sécurité. Le Comité était d'avis que cette différence

---

49 Il apparaît que l'intégrité de certains militaires peut effectivement poser problème. Cela signifie que ces militaires ne seront connus comme tels que lorsqu'ils représenteront une menace qui aura été détectée par le SGRS.

50 En ce compris les membres du service d'assistance religieuse et morale (SARM).

51 Les contrats Rosetta, ou 'Conventions de premier emploi', sont des contrats d'un an proposés à des jeunes de moins de 26 ans. La Défense organise elle-même les interviews de recrutement en fonction de ses besoins.

52 Par exemple, ceux qui sont recrutés ou détachés auprès du SGRS, étant donné que disposer d'une habilitation de sécurité constitue une des conditions essentielles pour pouvoir y travailler.

de traitement ne peut se justifier que si l'usage inapproprié de la fonction qu'ils occupent n'est pas susceptible de menacer les intérêts fondamentaux de l'État.

Le Comité permanent R soulignait également, à cet égard, les conséquences de l'évolution de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. En effet, outre une menace potentielle ou concrète dans un bâtiment ou un lieu, certains sites peuvent par nature (et en permanence) être sensibles aux menaces : le tarmac d'un aéroport, une base de la Défense, etc. L'utilisation inappropriée de la possibilité d'accéder à un tel lieu peut porter sérieusement atteinte aux intérêts fondamentaux de l'État. Il en va de même pour les personnes qui exercent une fonction ou mission particulière ou qui souhaitent obtenir une autorisation spécifique. Initialement, la loi permettait à « toute autorité administrative » d'exiger de tels avis (positifs).[53]

La Loi du 23 février 2018 et l'AR du 8 mai 2018[54] ont réformé la procédure d'avis de sécurité, que ce soit au niveau de la décision réglementaire de l'autorité administrative ou du mécanisme de décision individuelle.

I.7.2. LE SCREENING DE SÉCURITÉ POUR LES ÉTUDIANTS (ÉTRANGERS) DE L'ÉCOLE ROYALE MILITAIRE ?

L'École Royale Militaire (ERM) est une institution militaire d'enseignement universitaire destinée à la formation académique, militaire, et physique des futurs officiers, ainsi qu'à la formation continue d'officiers pendant leur carrière à la Défense.[55]

L'ERM ouvre également ses portes à des élèves étrangers. La Sûreté de l'État relevait que « *les universités sont en général ouvertes à la coopération internationale, ce qui constitue indéniablement une valeur ajoutée. Toutefois, cette ouverture n'est pas sans risque. D'autres acteurs savent que nos universités sont une véritable mine d'or. […] Des étudiants d'instituts de recherche militaire (tels que la Chinese National*

---

53 La décision (de nature réglementaire) de requérir un avis de sécurité (individuel) pouvait être prise « *lorsque l'exercice d'une profession, d'une fonction, d'une mission, d'un mandat ou l'accès à des locaux, des bâtiments, des sites, ou la détention d'un permis, d'une licence ou d'une autorisation pouvait, par un usage inapproprié, porter atteinte à la défense de l'intégrité du territoire national et des plans de défense militaire, à l'accomplissement des missions des forces armées, à la sûreté intérieure de l'État, y compris dans le domaine de l'énergie nucléaire, à la pérennité de l'ordre démocratique et constitutionnel, à la sûreté extérieure de l'État et aux relations internationales de la Belgique, au potentiel scientifique et économique du pays, à la sécurité des ressortissants belges à l'étranger ou au fonctionnement des Organes décisionnels de l'État* ».

54 Loi du 23 février 2018 portant modification de la loi L.C.&HS (*M.B.*, 1er juin 2018, p. 45591) et Arrêté royal du 8 mai 2018 modifiant l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (*M.B.*, 1er juin 2018, p. 45632).

55 L'ERM propose, entre autres, une formation de base (FBEM, anciennement appelée 'premier cycle'), une formation pour Candidat Officier supérieur (FCOS) ainsi qu'un Cours supérieur d'État-major (CSEM). Voir : www.rma.ac.be

University of Defense Technology) sont envoyés dans plusieurs pays d'Europe occidentale, dont la Belgique, pour y acquérir des connaissances essentielles à certains développements militaires. Ces étudiants et chercheurs emportent ensuite toutes les connaissances engrangées au sein des universités belges pour les mettre à disposition de l'armée de leur pays. À l'heure actuelle, quelques dizaines de ces étudiants militaires sont actifs dans des universités belges »[56].

Le Comité permanent R a également estimé que la Défense présentait une fragilité dans son accueil des élèves étrangers. Il existe en effet un risque non négligeable d'espionnage et d'ingérence dans le chef de certaines personnes qui, de surcroit, se voient offrir un accès à des informations de la Défense.

Par conséquent, l'admission d'étudiants étrangers nécessite, selon le Comité, une analyse de risque systématique et préalable au cas par cas (autrement dit de chaque candidat-élève) par le SGRS.

I.8. ENQUÊTE DE CONTRÔLE SUR LE SUIVI DES MANDATAIRES POLITIQUES

I.8.1. INTRODUCTION

Lors de débats (parlementaires) [57], une question est posée à maintes reprises, à savoir si et dans quelle mesure les services de renseignement belges suivent (ou sont autorisés à suivre) des mandataires politiques, et quelles règles doivent être observées à cet égard.[58] Depuis début janvier 2018, une note de service classifiée 'CONFIDENTIEL' est d'application au sein de la VSSE. Conformément à cette note, actualisée en juin 2020[59], le service envoie deux types de rapports au ministre de la Justice et au Premier ministre, avec copie au Comité permanent R. Il s'agit, d'une part, de rapports ponctuels sur des mandataires politiques qui contribueraient à l'apparition d'une menace et, d'autre part, d'un aperçu trimestriel de l'ensemble

---

56 https://www.vsse.be/sites/default/files/paragraphs/1-ra2020-fr-version10-single-light.pdf

57 Voir Question de S. Creyelman au ministre de la Justice sur les 'dossiers politiques à la VSSE' (*Q.R.* Chambre 2019-20, 16 juillet 2020, QRVA 23, 33, Q. n° 351).

58 COMITÉ PERMANENT R, *Rapport d'activités 2019*, 71-72 ('IV.3. Contrôle du suivi des mandataires politiques').

59 Cette note de service du 13 décembre 2017 a été actualisée en juin 2020 en vue d'améliorer les rapports destinés à la direction sur les activités disruptives. Malgré ses demandes répétées, le Comité n'a reçu, en 2019, aucune information du SGRS. Le Comité avait pourtant exhorté le SGRS, comme la VSSE d'ailleurs, à adopter une directive uniforme, assortie de règles claires et univoques quant au recueil, au traitement, à la consultation, au stockage et à l'archivage des informations relatives aux mandataires politiques. Le SGRS ne dispose pas d'une procédure spécifique pour traiter cette thématique, pas plus qu'il n'a défini de procédure pour informer le Comité permanent R.

des documents dans lesquels des mandataires politiques sont mentionnés.[60] Le ministre de la Justice avait marqué son accord sur le *« principe de vérifications par le Comité R qui s'avèrent nécessaires conformément à la loi organique du 18 juillet 1991 »*.[61]

Étant donné qu'il n'est mentionné nulle part ce que le Comité permanent R est censé faire des informations précitées, il a pris l'initiative de développer une méthodologie autour de cette problématique et de son rôle de contrôle. Cette méthodologie a été approuvée par la Commission parlementaire de suivi en 2020. Sur la base de cette méthodologie, une enquête de contrôle a été initiée en 2020 et finalisée en 2021.[62] L'enquête se penchait sur la fréquence avec laquelle, pendant la période de référence (du 1er septembre 2019[63] au 31 août 2020), des informations concernant un mandataire ont été recueillies, traitées et ont fait l'objet d'un rapport. Il s'agissait également de vérifier si la collecte d'informations était légale et non disproportionnée et si les recommandations formulées dans le passé par le Comité permanent R ont été exécutées. [64]

À cette fin, le Comité permanent R a établi une liste des (543) personnes ayant occupé, pendant la période de référence, un mandat politique au niveau européen, fédéral, régional et communautaire.[65]

Cette liste a été transmise fin octobre 2020 respectivement à la VSSE et au SGRS. En réponse, la VSSE a remis au Comité permanent R les listes des documents pertinents établis par ses services extérieurs et le service d'analyse. De son côté, le

---

60 Les mandataires politiques visés sont les ministres des différents gouvernements, le Commissaire belge siégeant à la Commission européenne et les membres des différents parlements et assemblées, y compris les membres belges du Parlement européen. Les autres élus ou mandataires désignés ne sont pas concernés (par ex. les échevins au niveau communal ou les gouverneurs au niveau provincial).

61 Voir le courrier du ministre de la Justice daté du 26 juillet 2018 et adressé au Comité permanent R sur 'le recueil d'informations par un service de renseignement concernant une personne exerçant un mandat politique'.

62 Le Comité permanent R a déjà mené des enquêtes sur ce sujet ou des matières connexes. Voir COMITÉ PERMANENT R, *Rapport d'activités 1998*, 60 et suiv. ; *Rapport d'activités 1999*, 13 et suiv. ; *Rapport d'activités 2008*, 20-21 et suiv. ; *Rapport d'activités 2013*, 3 ('I.I.3. Une nouvelle note de service de la VSSE sur le suivi des parlementaires').

63 Début de la législature fédérale parlementaire 55 (2019- 2024).

64 COMITÉ PERMANENT R, *Rapport d'activités 2013*, 37- 47 ('II.4. Le suivi de mandataires politiques par les services de renseignement').

65 Concrètement, il s'agissait : a) des ministres du Gouvernement flamand, du Gouvernement de la Fédération Wallonie-Bruxelles, du Gouvernement de la Région wallonne, du Gouvernement de la communauté germanophone, du Gouvernement bruxellois, du Gouvernement fédéral et des commissaires belges au sein de la Commission européenne ; b) des membres des parlements communautaires et régionaux (Fédération Wallonie-Bruxelles, Région wallonne, Région de Bruxelles-Capitale, Parlement flamand et communauté germanophone), du Parlement fédéral (Chambre et Sénat) et des membres belges du Parlement européen ; et c) à l'exception des présidents de partis politiques qui ne sont pas membres d'un parlement et n'ont pas de mandat exécutif à l'un des niveaux susmentionnés, des membres de la famille royale, des ministres d'État, des mandataires locaux (bourgmestres, échevins, conseillers communaux, membres d'intercommunales) pour autant qu'ils ne revêtent aucun mandat régional/communautaire/fédéral/européen, des gouverneurs et anciens mandataires sans mandat actuel.

SGRS a signalé au Comité que le service n'avait suivi ni examiné aucun mandataire politique belge pendant la période de référence.

I.8.2. CONSTATATIONS CONCERNANT L'EXÉCUTION DES RECOMMANDATIONS FORMULÉES PAR LE COMITÉ PERMANENT R

I.8.2.1. L'élaboration de directives quant au recueil, au traitement, à la consultation, au stockage et à l'archivage des données

En 2008, le Comité permanent R avait recommandé l'élaboration de directives claires et non équivoques quant au recueil, au traitement, à la consultation (y compris le cloisonnement interne éventuel), au stockage et à l'archivage des données de certaines catégories de personnes qui assument ou ont assumé des responsabilités particulières.[66]

En juin 2020, la VSSE a produit une note de service[67] qui définit de nouvelles directives internes et actualise les procédures, en remplacement de trois notes de services antérieures.[68] Cette note prévoit notamment « *l'obligation de notification de la VSSE au ministre de la Justice dès que certains mandataires politiques apparaissent dans les documents de la VSSE* ». Début décembre 2020, la VSSE a en outre envoyé une note aux partis politiques représentés au sein du Parlement fédéral expliquant la procédure suivie lorsque les noms de mandataires politiques apparaissent dans le cadre d'enquêtes de la VSSE.[69]

Malgré les recommandations formulées en 2013[70], le Comité permanent R n'a reçu du SGRS aucune information selon laquelle il prévoyait une procédure

---

66 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 110 et suiv. (VIII.1.2. Des directives pour le traitement de données concernant certaines catégories de personnes.)

67 VSSE, Note de service du 11 juin 2020.

68 La note de service du 4 juillet 2013 ayant pour objet « *Modifications pour l'établissement de documents sauvegardés dans VESTA* », la note de service du 25 juillet 2013 intitulée « *Note de service concernant les liens de parlementaires et mandataires politiques dans les documents de la VSSE* » et la note de service du 13 décembre 2017 concernant « *l'obligation de notification de la VSSE au ministre de la Justice dès que certains mandataires politiques apparaissent dans les documents de la VSSE* ».

69 Procédure mandataires politiques concernant : *'la mention d'un mandataire politique dans la base de données de la VSSE', 'si le mandataire politique est la victime d'une menace', 'l'implication présumée ou avérée d'un mandataire politique dans l'apparition d'une menace'*.

70 COMITÉ PERMANENT R, *Rapport d'activités 2013*, 112 ('IX.1.2. Une directive sur le travail de renseignement à l'égard de personnes exerçant des responsabilités particulières et de partis politiques' et 'IX.1.3. « Directives univoques concernant l'information sur le suivi des responsables politiques').

spécifique pour la gestion de ces informations, et aucune procédure n'a été déterminée pour informer le Comité permanent R.[71]

I.8.2.2. Une attention particulière pour la position des mandataires politiques mentionnés

Une recommandation antérieure du Comité portait sur l'attention nécessaire à accorder à la position, vis-à-vis de la menace (victime, acteur, passant, etc.), des mandataires politiques mentionnés dans les rapports des services de renseignement. Les mandataires politiques peuvent, par exemple, apparaitre dans le radar des services de renseignement via des informations récoltées dans le cadre de l'exercice de leur mandat ou en marge d'une menace : ils peuvent être cités par des sources humaines, apparaître dans des messages de services partenaires, figurer dans des listes créées suite à l'application de ressources techniques (par ex. listes de téléphonie). Dans de tels cas, le mandataire politique entre fortuitement dans le champ de vision des services de renseignement.

Ainsi, la note de service de la VSSE stipule que les mandataires politiques qui apparaissent dans des documents de la VSSE ne peuvent être « reliés » à la menace que s'ils apparaissent comme victimes ou auteurs au sens de la L.R&S.

---

[71] Le 30 novembre 2017, le SGRS signalait au Comité permanent R que depuis les recommandations de 2013, la Loi organique de 1998 avait été modifiée à plusieurs reprises, constatant qu'aucune autorité politique ou législative n'avait admis avoir connaissance du fait que de telles règles devaient être établies concernant le suivi des responsables politiques. Le suivi de responsables politiques par le SGRS n'avait, selon lui, pas porté préjudice à la liberté d'association ou d'expression et, si cela avait été le cas, il y aurait été procédé sur la base de la Loi organique qui est en conformité avec la Déclaration universelle des droits de l'homme et avec les arrêts de la Cour européenne des droits de l'homme, dans le sens où il est prévu que dans certaines situations correctement décrites, il est possible d'aller à l'encontre de l'un ou l'autre droit fondamental. En dépit de cette constatation, le SGRS estimait que toutes les initiatives capables de consolider les contrôles démocratiques sur les services de renseignement devaient être encouragées et que le SGRS pouvait lui aussi jouer un rôle crucial dans cette consolidation. Dans cette optique, le SGRS a pris l'initiative de contacter la VSSE pour réfléchir à la (aux) recommandation(s) prise(s). Le SGRS a également signalé en date du 6 décembre 2017 au Comité permanent R qu'il avait l'intention d'élaborer dans le courant de 2018 des procédures similaires à celles de la VSSE pour informer les organes de contrôle démocratiques, dans le sens où l'élaboration de telles procédures devait également être liée à l'élaboration de procédures internes concernant la sauvegarde et l'archivage d'informations concernant les mandataires et organisations politiques concernés. L'élaboration de ces procédures devait s'inscrire dans le cadre d'un projet plus vaste qui prévoit la rédaction de plusieurs directives internes pour le fonctionnement du personnel(-cadre) du SGRS. L'audit du Comité permanent R sur le fonctionnement de la Direction CI et du SGRS, réalisé en février et mars 2018, et la publication des résultats de cet audit le 15 mai 2018, contrariaient les plans du SGRS pour l'élaboration desdites procédures. Le SGRS a cependant estimé qu'il était judicieux d'attendre les conclusions du Business Process Re-engineering (BPR), le processus de réforme interne du SGRS mis en place à l'issue de l'audit du Comité permanent R. Le 6 janvier 2020, le SGRS mettait en place sa nouvelle structure.

Il ressort toutefois de l'examen des documents visés que le rôle joué (victime, acteur, passant, etc.) par les mandataires politiques mentionnés n'était pas décrit de manière suffisamment claire.

I.8.2.3. L'exécution de l'article 19 L.R&S.[72]

La note de service susmentionnée précise qu'un aperçu de tous les documents dans lesquels figurent des mandataires politiques est transmis tous les trois mois par la VSSE au Comité permanent R (voir *infra*). L'aperçu reprend les références des documents qui contiennent des informations brutes ainsi que les références des documents d'analyse. L'aperçu indique également quelles notes ont été transmises au ministre de la Justice et au Premier ministre.[73]

En ce qui concerne le SGRS, le Comité permanent R recommande au service de lui remettre tous les trois mois un aperçu de tous les documents dans lesquels des mandataires politiques sont mentionnés.

I.8.3. LA COLLECTE, L'ANALYSE ET LA DIFFUSION DES RENSEIGNEMENTS SUR LES MANDATAIRES POLITIQUES ENTRE 2019 ET 2020

I.8.3.1. Collecte et analyse

Pendant la période de référence, sur les 543 mandataires politiques :
- 49 % (267) n'étaient pas repris dans la base de données de la VSSE ;
- 23 % (124) étaient repris dans la base de données de la VSSE, mais sans lien avec une menace ;
- 28 % (152) étaient repris dans la base de données de la VSSE, avec mention dans des documents d'analyse (828) produits par la VSSE à propos d'une menace.

Sur ces 828 documents d'analyse, 53 % (439) sont des rapports d'enquête, 25 % (206) des documents transmis par un partenaire (inter)national externe, 6 % (53)

---

72 « Art. 19 L.R&S : *Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une menace visée aux articles 7 et 11.*
Dans le respect de la vie privée des personnes, et pour autant que l'information du public ou l'intérêt général l'exige, l'administrateur général de la Sûreté de l'État et le chef du Service général du renseignement et de la sécurité, ou la personne qu'ils désignent chacun, peuvent communiquer des informations à la presse. »

73 Le ministre de la Justice et le Premier ministre ne sont pas informés d'une mention purement accidentelle de mandataires politiques dans des documents de la VSSE.

des notes aux autorités belges et 16 % (130) des documents divers (essentiellement des procès-verbaux de réunions et des fiches de synthèse élaborées dans le cadre de l'analyse interne d'un dossier).

I.8.3.2. Diffusion des renseignements

La VSSE remet chaque trimestre au Premier ministre et au ministre de la Justice, avec copie au Comité permanent R, un aperçu de tous les documents dans lesquels apparaissent des mandataires politiques.

En outre, dès que, sur la base des informations disponibles, il y a une présomption d'implication d'un mandataire politique dans l'apparition d'une menace, le ministre de la Justice et le Premier ministre, avec notification au Comité permanent R, en sont informés via des fiches de notification. Ces fiches sont éventuellement complétées par le détail des informations analysées et vérifiées qui justifient la notification des autorités. Pendant la période de référence, cinq fiches de notification de ce genre ont été établies pour autant de mandataires.

La VSSE partage en outre les informations à propos des mandataires politiques dont le nom apparait dans certains documents sans toutefois pouvoir être reliés à une menace. Dans des notes aux autorités, la VSSE fournit ainsi une description de la manière dont le mandataire politique contribue à l'apparition d'une menace, une évaluation des possibles conséquences que peut ou a pu avoir cette implication (pour autant qu'elles soient connues) et la manière dont le dossier sera traité.

Pendant la période de référence, 17 des 543 mandataires politiques (3,13 %) ont fait l'objet de 53 notes aux autorités (21 concernant l'extrémisme, 25 pour espionnage et ingérence, 7 autres tels que organisations criminelles ou corruption).[74]

I.8.4. LE RESPECT DES DROITS FONDAMENTAUX DES MANDATAIRES POLITIQUES

La légalité du recueil des informations repose sur la(es) mission(s) des services de renseignement telle(s) que précisée(s) à l'article 7 L.R&S.

Le Comité permanent R n'a trouvé aucune indication selon laquelle la VSSE visait des mandataires politiques pour des raisons étrangères aux intérêts et menaces énumérés dans la loi, ni qu'ils étaient traités différemment des autres groupes professionnels.

---

[74] L'examen des 53 notes aux autorités belges (NA) susmentionnées indique qu'elles étaient également adressées à l'une ou plusieurs des personnes/institutions suivantes selon le principe du '*need to know*' : Comité permanent R (28), OCAM (13), Police fédérale (13), SGRS (12), ministre de la Justice (9), Parquet fédéral (9), Direction générale du centre de crise (6), Procureur du Roi (5), Premier ministre (5), autres (24 – par exemple, Direction générale des Établissements pénitentiaires, Cellule de traitement des informations financières, SPF Intérieur ou Police locale).

De l'examen des notes aux autorités, il ne ressort pas que les droits fondamentaux des mandataires politiques n'ont pas été respectés dans le recueil, l'analyse et la diffusion d'informations.

Sur la base des critères repris dans la méthodologie approuvée par la Commission de suivi, il ne ressort pas de l'enquête que des mandataires politiques apparaissent de manière disproportionnée dans les documents de la VSSE.

I.9. ENQUÊTE SUR LA DÉTECTION ET LE SUIVI DE LA RADICALISATION D'UN MILITAIRE DE LA DÉFENSE : L'AFFAIRE JÜRGEN CONINGS

En mai 2021, Jürgen Conings, fiché comme 'extrémiste potentiellement violent' (EPV)[75] par l'OCAM, a quitté la caserne de Bourg-Léopold et a pris la fuite en emportant des armes. Au moment de sa disparition, l'intéressé était employé comme Caporal-chef à la Défense. Il est apparu rapidement que l'intéressé était connu des services de police et des services de renseignement et de sécurité (voir *infra*). L'affaire a ému l'opinion publique et a soulevé, à juste titre, de très nombreuses questions (parlementaires).[76]

Sur demande de la ministre de la Défense, le Comité permanent R a ouvert une *'enquête de contrôle concernant, d'une part la détection et le suivi de la radicalisation d'un militaire de la Défense par les deux services de renseignement, et d'autre part, leur collaboration portant notamment sur l'échange d'informations avec leurs partenaires, y compris avec la Défense'*. À travers cette enquête, la ministre de la Défense a assigné trois missions au Comité : (a) vérifier la fiabilité des informations relatives aux personnes suspectées de radicalisation au sein de la Défense, (b) coopérer avec l'inspecteur général de la Défense chargé de réaliser un audit portant notamment sur les aspects de la gestion du personnel et (c) formuler des recommandations en vue de garantir le bon fonctionnement du SGRS, mais aussi de la Défense dans son ensemble.

En ce qui concerne le rôle de l'OCAM dans cette affaire, une '*enquête de contrôle commune sur le rôle de l'OCAM et ses services d'appui, dans le suivi de Jürgen Conings, notamment dans sa mise en « pré-enquête », de son évaluation au*

---

75 Les EPV sont l'une des catégories de la banque de données commune *Terrorist Fighters* dont l'OCAM est le gestionnaire opérationnel. Les entités inscrites comme EPV doivent remplir une série de critères définis dans l'A.R. du 20 décembre 2019 modifiant l'A.R. du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters et l'A.R. du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1er*bis* « de la gestion des informations » du chapitre IV de la loi sur la fonction de police, *M.B.* 27 janvier 2020. Voir COMITÉ PERMANENT R, *Rapport d'activités 2020*, 128 ('VI.1.1. L'ajout des extrémistes potentiellement violents (EPV) dans la BDC TF').

76 Voir, par exemple, le Débat d'actualité sur le militaire en fuite (Commission de la Défense nationale), *C.R.I.* Chambre 2020-21, 26 mai 2021, COM 490 et les débats autour du rapport de l'Inspecteur général, *C.R.I.* Chambre, 2020-2021, 16 juin 2021, COM 519.

niveau 3 de la menace et de ses conséquences, et sur l'échange d'informations relatif à cette personne' a été initiée conjointement avec le Comité permanent P.[77]

Les rapports d'enquête ont été discutés début juillet 2021 avec la Commission parlementaire de suivi.

I.9.1. UN APERÇU DU PARCOURS PROFESSIONNEL DE JÜRGEN CONINGS

Le parcours professionnel de Jürgen Conings est fait d'un enchevêtrement d'affectations, de mutations, de missions à l'étranger[78], de formations en tous genres[79] au sein de la Défense ainsi que de petits boulots dans le secteur de la sécurité privée. Démarrée en 1992, la carrière du militaire est ainsi ponctuée par plusieurs changements d'affectation jusqu'à sa mutation, à sa demande, en juin 2020 au sein de la Cellule *Pre-Deployment Training for Individual Augmentees* (PDT-IA[80]) en tant que collaborateur logistique, réparateur d'armes et instructeur auxiliaire.

S'il apparait dans les radars de la Sûreté de l'État pour la première fois en 2015, l'intéressé obtient toujours de 'bonnes' évaluations au sein de la Défense, et ce malgré une sanction (un arrêt simple de quatre jours) pour propos racistes tenus sur Facebook en novembre 2019. [81] Le rapport de l'Inspection générale de la Défense fait également mention de facteurs psychosociaux.[82]

En mars 2020, il postule à la Police fédérale pour une fonction d'agent de sécurité mais sera recalé sur la base de son test de personnalité. En parallèle de ses affectations au sein de la Défense, il continue néanmoins son parcours dans le secteur de la sécurité privée en tant qu'agent de gardiennage.

Le 31 août 2020, son habilitation de sécurité n'est pas prolongée. Le même jour, il est inscrit par l'OCAM en pré-enquête EPV. Le 17 février 2021, il se voit

---

77 Voir 'I.10 Enquête commune de contrôle sur le rôle de l'OCAM dans le suivi du militaire Jürgen Conings'. Dans un souci d'exhaustivité, ces deux rapports d'enquête doivent être lus conjointement.

78 Entre autres, en ex-Yougoslavie (BELBAT), en Afghanistan (Resolute Support Mission) et en Jordanie (Operation Desert Falcon).

79 Entre autres, des formations au matériel roulant, des formations techniques (gestion d'entrepôt, réparation de radios, etc.) et des cours d'armement.

80 Cette cellule de la Composante Terre est responsable de la préparation des militaires de l'ensemble de la Défense qui, en tant qu'individu, participeront à des opérations (par exemple, les militaires impliqués dans certaines missions, indépendamment d'un grand détachement lié à leur propre unité, voire à leur composante).

81 Le motif avancé est le suivant : *"Betrokkene heeft op sociale media een mening geuit die niet strookt met de waarden van Defensie en schade toebrengt aan het imago van Defensie"*. L'intéressé a exprimé dans les médias sociaux une opinion qui n'est pas conforme aux valeurs de la Défense et qui porte atteinte à son image (traduction libre).

82 Inspectoraat-generaal, Eindrapport E2103. Intern onderzoek PDT-IA, Beperkte verspreiding.

attribuer le *full* statut d'EPV niveau 3[83] (art. 6, § 1er, 1°/2 AR TF). Le 3 mars 2021, sa promotion sociale est annulée. Le 17 mai 2021, il quitte la caserne en possession d'armes avant que sa disparition soit signalée le lendemain. Le 21 mai 2021, un juge d'instruction a été désigné pour 'tentative d'assassinat dans un contexte terroriste' et 'possession illégale d'armes dans un contexte terroriste'. Une procédure de suppression d'emploi a été lancée. Le 20 juin 2021, soit cinq semaines après sa disparition, il a été retrouvé sans vie.

Jürgen Conings faisait ainsi partie des quelque 30[84] militaires suivis par le service de renseignement militaire pour leur proximité avec les milieux d'extrême droite.[85] À sa disparition, il a d'ailleurs reçu le soutien de Tomas Boutens, ancien militaire et leader du groupe néo-nazi *Bloed, Bodem, Eer & Trouw*.[86] Sur un de ses profils Facebook, Jürgen Conings avait fait référence au 'Siegrune', un symbole runique utilisé dans l'Allemagne nazie. Plus encore que les contacts sporadiques avec Boutens, il avait été remarqué dans les milieux de la *Vlaams Legioen*[87], où il aurait donné un entraînement au combat. Jürgen Conings faisait également partie du groupe Facebook des *Knights of Flanders*, un groupe d'extrême droite.

I.9.2. CADRE JURIDIQUE ET POLITIQUE

Avant d'évaluer la position d'information des services de renseignement concernant Jürgen Conings, il importait de clarifier les compétences de la VSSE et du SGRS dans le cadre de la détection, du suivi et de la lutte contre le terrorisme, l'extrémisme et le radicalisme.

---

83 Conformément à l'article 11 de l'A.R. du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, l'OCAM travaille à partir d'une échelle de quatre niveaux de la menace (du niveau 1 'faible' au niveau 4 'très grave'). Le niveau 3 rend compte d'une menace 'grave'.

84 À titre de comparaison, les services de police suivent environ 2500 personnes dans les milieux d'extrême droite.

85 L'influence exercée par l'extrême droite dans les rangs militaires n'est pas un phénomène uniquement belge, pas plus qu'il n'est nouveau. Au sein de l'unité d'élite allemande *Kommando Spezialkräft* (KSK), cinquante militaires sont suspectés depuis 2017 de mener des activités d'extrême droite. Récemment, un coup d'État mené par un ancien général issu des cercles de la droite (extrême) a suscité des craintes. Aux Pays-Bas aussi, plusieurs militaires ont quitté les forces armées ces cinq dernières années après avoir tenu des propos ou adopté un comportement d'extrême droite. Fin des années 90, l'ancien ministre de la Défense avait déjà prévenu qu'un bataillon de paras près d'Anvers ne devait pas être affecté par des tendances fascistes et racistes.

86 Condamné à cinq ans de prison pour avoir planifié, avec seize autres personnes appartenant pour la plupart à l'Armée belge des actes terroristes et diffusé une idéologie faisant l'apologie de la violence (deux tiers des individus arrêtés à l'époque étaient des militaires de carrière), Tomas Boutens a été l'un des premiers à avoir affiché son soutien au fugitif sur Facebook.

87 Un groupuscule d'extrême droite qui 'lutte pour le peuple flamand et pour la Flandre'.

I.9.2.1. Les missions de renseignement de la VSSE et du SGRS

L'assignation des tâches de la VSSE dans la lutte contre le terrorisme, l'extrémisme et le radicalisme se situe à titre principal dans le cadre de sa mission de renseignement (art. 7, 1° L.R&S). Le législateur a choisi d'établir une liste limitative des menaces contre la sécurité qui relèvent du domaine de compétence de la VSSE. L'article 8, 1°, alinéas 2, b et c L.R&S définit les menaces visées par l'enquête de contrôle, à savoir le terrorisme et l'extrémisme (en ce compris le processus de radicalisation).

Les activités du SGRS en matière de terrorisme, d'extrémisme et de radicalisme se situent elles aussi à titre principal dans le cadre de sa mission de renseignement telle que définie à l'article 11, § 1er, 1° L.R&S. À l'instar de la VSSE, le SGRS doit sauvegarder certains intérêts fondamentaux du pays au moyen de la détection, du suivi et de la lutte contre certaines menaces pesant sur ces intérêts. La principale différence réside dans la présence requise d'un aspect militaire, soit dans l'intérêt à protéger (par ex. les plans de défense militaires, l'exercice des missions militaires), soit la manière dont les intérêts à protéger peuvent être affectés, c'est-à-dire par des moyens de nature militaire (par ex. des armes militaires, du personnel de la Défense).

Les renseignements obtenus par les deux services, c'est-à-dire les informations collectées et analysées, sont ensuite tranmises à d'autres instances, en temps utile et de manière ciblée.[88] Ces instances (principalement politiques, administratives, judiciaires, policières, diplomatiques et militaires) prennent *in fine* les contre-mesures nécessaires pour protéger la sécurité nationale.

Cette vaste mission légale de renseignement impose aux services et à leurs responsables politiques de définir des priorités dans le cadre de leurs activités. En effet, la VSSE et le SGRS ne disposent pas des capacités et des moyens suffisants pour détecter, suivre et maîtriser (ni n'auraient jamais pu) toutes les menaces nationales en matière de sécurité relevant de leur compétence. Cette mission de priorisation incombe au Conseil national de sécurité (CNS).[89]

Le CNS est également chargé de définir les modalités de coopération effective entre les différents services de sécurité. A cette fin, le Plan Stratégique National du Renseignement (PSNR), établi conjointement par la VSSE et le SGRS et validé par le CNS en 2018, *'entend'*, entre autres, *'optimiser la coopération entre les services*

---

88 En vertu de l'article 19 L.R&S, les destinataires des renseignements sont les '(…) *ministres et autorités administratives et judiciaires concernés, (…) services de police et (…) toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi que (…) instances et personnes qui font l'objet d'une menace visée aux articles 7 et 11*'. Les destinataires des informations des services de renseignement sont donc certaines instances publiques politiques, administratives, judiciaires, policières, diplomatiques et militaires. Des informations utiles peuvent également être portées à la connaissance de personnes ou d'instances menacées (par ex. un employeur).

89 Tel que confirmé à la lecture des articles 4 et 10 L.R&S et de l'article 2 de l'A.R. du 22 décembre 2020 portant création du Conseil national de sécurité, du Comité stratégique du renseignement et de la sécurité et du Comité de coordination du renseignement et de la sécurité, *M.B.* 29 décembre 2020.

de renseignement afin de mettre en oeuvre une politique de renseignement la plus efficiente possible en faveur des autorités compétentes et de la population.'.[90] Dans la section (classifiée) « Répartition des tâches », le PSNR détaille les compétences respectives de la VSSE et du SGRS en matière de lutte contre le terrorisme, l'extrémisme et le radicalisme.

I.9.2.2. La réalisation de screenings de sécurité par les deux services de renseignement

Outre leurs missions de renseignement, la VSSE et le SGRS ont également des missions de sécurité, au premier rang desquelles il convient de citer la réalisation de screenings de sécurité.
Les deux services mènent en effet des enquêtes de sécurité, c'est-à-dire les enquêtes effectuées au service d'une autorité de sécurité (principalement l'ANS) afin de vérifier si une personne satisfait aux conditions en matière de secret, loyauté et intégrité. Ces conditions sont nécessaires pour obtenir ou conserver une habilitation de sécurité.[91] Les services de renseignement sont en outre chargés de réaliser les vérifications de sécurité en vue de l'octroi d'une attestation ou d'un avis de sécurité.
Au sein des Forces armées, le SGRS remplit également la fonction d'autorité de sécurité. Ceci signifie qu'il est aussi chargé, en plus de la réalisation des enquêtes et des vérifications de sécurité, de l'octroi des habilitations et des avis de sécurité. Le Comité constate toutefois qu'au sein des Forces armées, il n'existe aucune instruction générale énumérant de manière exhaustive les fonctions à la Défense qui requièrent une habilitation de sécurité.
En vertu de la Loi du 28 février 2007 fixant le statut des militaires du cadre actif des Forces armées, un avis de sécurité positif est par contre exigé pour tout candidat-militaire (cf. art. 9, 9°). La loi n'impose cependant pas de screening de sécurité périodique pour les militaires.[92]

---

90 Plan Stratégique National du Renseignement, 4.

91 Les enquêtes de sécurité sont effectuées conformément aux directives (datées et peu adaptées) du 16 février 2000 du Comité ministériel du renseignement et de la sécurité (devenu le Conseil national de sécurité). Le Comité rappelle l'urgence d'actualiser les directives du Comité ministériel du renseignement et de la sécurité portant sur toutes sortes de règles de sécurité (portée des enquêtes de sécurité, règles de classification, conservation des pièces classifiées, infosec, missions des officiers de sécurité). Les directives en question remontent toutes à 2001 et nécessitent une adaptation.

92 Voir 'I.7. Les screenings de sécurité des militaires et et des civils à la Défense'.

I.9.2.3. La responsabilité du SGRS en matière de sécurité militaire[93]

Outre la réalisation d'enquêtes et de vérifications de sécurité, le SGRS est également chargé *'de veiller au maintien de la sécurité militaire du personnel relevant du Ministre de la Défense nationale, et des installations militaires, armes et systèmes d'armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires'* (art. 11, § 1er, 2° L.R&S). La notion de sécurité militaire englobe donc, en plus de la sécurité des renseignements, *'la sécurité des personnes, du matériel et des installations'*.[94]

Ainsi, plusieurs directives ont été établies et diffusées par le SGRS en la matière et réglementent, par exemple, le stockage des armes et des munitions (les règlements IF5 et IF5(bis)).[95] Les compétences du SGRS consistent ici à conseiller le commandement militaire sur les mesures de protections adéquates, à vérifier leur mise en œuvre, à constater les éventuelles lacunes, à informer le commandement militaire précité des défaillances constatées et à formuler les recommandations requises pour y remédier.

I.9.3. LES CONSTATATIONS DE L'ENQUÊTE

L'affaire Conings illustre les constatations du Comité permanent R au fil des enquêtes de contrôle qu'il a effectuées ces dernières années. Cette affaire apparait comme étant le point d'intersection de toutes les constatations antérieures, en particulier en ce qui concerne le service de renseignement militaire. Les recommandations qui y sont associées conservent elles aussi toute leur valeur d'actualité,[96] tout

---

93 Le Comité rappelle qu'en 1999 et 2003 déjà – chaque fois à la suite d'un vol conséquent d'armes et/ou de munitions sur un site militaire – il avait fait état d'une enquête de contrôle ouverte en rapport avec ces incidents. Ces enquêtes étaient relatives respectivement à *'l'efficacité du SGR et à la collaboration des deux services de renseignement concernant le vol d'armes commis à Houthulst en 1997'* (COMITÉ PERMANENT R, *Rapport d'activités* 1999, 74 et suiv.) et à *'la sécurité et à la surveillance d'un dépôt militaire d'armes (Thuin)'* (COMITÉ PERMANENT R, *Rapport d'activités 2003*, 192 et suiv.).

94 Projet de loi organique des services de renseignement et de sécurité, *Doc. parl.*, Chambre 1995-1996, n°49-638/001, 11-12.

95 Le SGRS a informé le Comité permanent R à plusieurs reprises ces dernières années que le Règlement IF5(bis) serait actualisé. La version la plus récente du Règlement qui a été transmise au Comité est celle de 2016. Le Comité n'a pas connaissance d'une version plus actuelle.

96 Voir par exemple COMITÉ PERMANENT R, *Rapport d'activités 2020*, 38-53 ('Le suivi de l'extrême droite par les services de renseignement belges' ; *Rapport d'activités 2019,* 2-13 ('La réalisation de screenings de sécurité par les services de renseignement') ; *Rapport d'activités 2016,* 70-73 ('Évaluations individuelles de la menace par l'OCAM') ; *Rapport d'activités 2011,* 7-14 ('Un audit au sein du service de renseignement militaire') et 25-33 ('Les flux d'informations entre l'OCAM et ses services d'appui').

comme celles qui ont été formulées par la Commission d'enquête parlementaire 'Attentats'.[97]

I.9.3.1. La position d'information de la VSSE

Jürgen Conings est entré pour la première fois dans les radars de la Sûreté de l'État en septembre 2015 dans le cadre d'une récolte de fonds sur Facebook pour Dwekh Nawsha, une organisation paramilitaire chrétienne créée en soutien à la communauté assyrienne en Irak contre l'État islamique.[98] Il a attiré une seconde fois l'attention de la VSSE en octobre 2018.

Dans les deux documents de 2015 et 2018, il est mentionné que l'intéressé est un militaire. Le Comité permanent R a constaté que la VSSE n'avait pas partagé l'information de 2015 avec le SGRS, ne la considérant pas assez pertinente. L'information de 2018 a été communiquée au SGRS lors d'une réunion du Groupe de travail Extrême droite (Plan d'action Radicalisme ou Plan R)[99], au cours de laquelle les noms de l'organisation et des principaux protagonistes ont été mentionnés en termes généraux. Cette information a été communiquée à l'OCAM en 2020.

Entre juillet 2020 et mai 2021, la VSSE a rédigé plusieurs rapports d'information, dans lesquels étaient mentionnés la participation de Conings à des activités des groupements d'extrême droite *Knights of Flanders* et *Vlaams Legioen*. La VSSE a en outre constaté que Conings était en contact avec Tomas Boutens, l'ancien militaire et leader du groupuscule néo-nazi *Bloed, Bodem, Eer en Trouw* condamné en 2014 pour des faits de terrorisme.

Fin juin 2020, la VSSE a transmis une note à l'OCAM, au Parquet fédéral et au SGRS, entre autres, dans laquelle elle faisait mention d'un profil Facebook extrémiste de Conings et des menaces proférées par ce dernier à l'encontre du virologue Marc Van Ranst. En août 2020, la VSSE pose une série de questions spécifiques au SGRS. Pour autant que le Comité permanent R a pu le vérifier, le SGRS n'a jamais répondu officiellement à ces questions de la VSSE.

I.9.3.2. La position d'information du SGRS

Dès juillet 2020, peu après que des informations policières ont relié Conings aux possibles menaces à l'encontre de Marc Van Ranst, il a été signalé au sein du SGRS que l'intéressé devait retenir davantage l'attention. Le SGRS n'a pas communiqué ces informations à l'OCAM à ce moment-là, bien qu'une pré-enquête était en

97 *Doc. parl.*, Chambre, 2016-17, 54-1752/008 (15 juin 2017).

98 Selon des sources ouvertes, des *foreign fighters*, provenant, entre autres, des États-Unis, de France, du Royaume-Uni et d'Australie auraient rallié Dwekh Nawsha.

99 Devenu Stratégie Extrémisme et Terrorisme' (Stratégie TER) en septembre 2021.

cours concernant Conings dans le cadre de sa potentielle inscription comme EPV dans la BDC TF.

En février 2021, le SGRS valide une opération de renseignement avec Conings parmi les cibles, c'est-à-dire la mise en œuvre de méthodes de recueil de données (MRD). L'enquête du Comité permanent R a cependant montré qu'aucune MRD n'avait été mise en oeuvre jusqu'au 17 mai 2021. Le SGRS explique ce retard par une charge de travail élevée et l'absence de collaborateurs responsables de la gestion des MRD.[100]

L'intervention de la VSSE n'a pas été sollicitée en la matière, vu qu'il s'agissait d'un militaire.

Au cours des entretiens menés par le Comité, il est également apparu que les collaborateurs du SGRS ne sont pas, ou à peine, familiarisés avec l'utilisation et la finalité de la BDC TF.[101]

En outre, malgré la cinquantaine de collaborateurs du SGRS ayant un accès direct à la BDC TF, une trentaine de loggings enregistrés entre novembre 2020 et avril 2021 ont été effectués par seulement quelques collaborateurs.[102] Concernant Jürgen Conings plus spécifiquement, la fiche de renseignements de l'intéressé a été consultée le 15 janvier et le 19 février 2021 (le 17 février, il est passé en niveau 3). L'opération susmentionnée validée en février 2021 concernant Conings n'est toutefois pas liée à son évaluation au niveau 3 de la menace par l'OCAM.

L'enquête montre que l'existence du Plan R et de la BDC TF ne sont pas pris en considération au sein du SGRS. Il ressort de l'examen du dossier que ni la pré-enquête EPV, ni l'inscription comme EPV dans le BDC TF, ni l'évaluation au niveau de menace à 3 par l'OCAM n'ont eu d'impact sur le suivi de l'intéressé par le service de renseignement militaire.

Le SGRS a également manqué à ses obligations vis-à-vis du fonctionnement de la LTF.[103] Après la mise en pré-enquête de l'intéressé dans la BDC, le SGRS n'a fourni aucune information complémentaire et n'a pas joué son rôle d'initiateur

---

100 Lorsque des collaborateurs sont absents ou empêchés, leur remplacement n'est pas automatiquement prévu. Ainsi, il pouvait arriver que l'opération autour de Conings accuse un retard en raison, entre autres, d'une absence pour maladie du *case manager* qui devait gérer l'opération, et que personne au SGRS n'était présent à une réunion cruciale de la LTF compétente le 24 février 2021 au cours de laquelle ont été communiquées l'inscription de Conings comme EPV dans la BDC TF et l'attibution du niveau 3 de la menace par l'OCAM.

101 Ils ne sont pas au courant de la signification et des conséquences de l'inscription d'une entité dans une des catégories de la BDC TF et du niveau de menace attribué à une telle entité. Pour eux, l'inscription d'une entité ne change rien au suivi de celle-ci au niveau du travail de renseignement.

102 Il ressort néamoins des entretiens que personne de l'analyse, de la collecte ni de la hiérarchie n'était au courant que Jürgen Conings était repris dans la BDC TF, donc pas non plus du fait qu'à la fin février 2021, Jürgen Conings était fiché comme EPV avec une mention du niveau 3.

103 Autre problème : les réunions de la LTF compétente au début de la pandémie de COVID 19 ont été suspendues pendant un certain temps (mars et avril 2020) et se sont tenues par la suite en mode 'hybride' (certains services étaient physiquement présents aux réunions, tandis que d'autres services participaient par vidéoconférence). Compte tenu de la communication non sécurisée via les vidéoconférences, aucune information classifiée ne peut être échangée entre les participants.

(pourtant attendu compte tenu de la qualité de militaire de l'intéressé) dans un débat sur d'éventuelles mesures à prendre. À la réunion du 24 février 2021 de la LTF compétente, lors de laquelle l'inscription de Conings dans la BDC TF et le niveau 3 ont été communiqués, le SGRS n'était pas réprésenté.

I.9.3.3. Un manque de communication

Outre certains dysfonctionnements dans la communication avec la VSSE[104] et l'OCAM[105] abordés dans le rapport d'enquête, l'affaire Jürgen Conings a mis en lumière la persistance de problèmes de communication au sein même du SGRS. Ces défis en matière de communication interne avaient déjà été identifiés lors d'enquêtes de contrôle antérieures ainsi que par la Commission d'enquête parlementaire 'Attentats'. Ils avaient fait l'objet de recommandations.

La nouvelle structure du SGRS, élaborée en janvier 2020 en réponse à ces recommandations, n'a pas (encore) permis de résoudre les problèmes du passé. L'enquête a montré que les collaborateurs des échelons hiérarchiques inférieurs du SGRS perçoivent la structure actuelle du service comme complexe et peu claire. Le flou règne en ce qui concerne les compétences et la chaine de communication.

En outre, le Comité a pu observer qu'au sein de la plateforme PF6, en charge du suivi de l'extrême droite, des problèmes parmi les membres du personnel étaient survenus entre juillet 2020, alors que Jürgen Conings fait l'objet d'une attention particulière en raison des menaces qu'il a proférées à l'encontre du virologue Marc Van Ranst, et février 2021, au moment où l'intéressé a été repris dans la BDC TF.

Il y a également beaucoup d'incertitudes autour du fonctionnement précis du *Defence Intelligence & Security Command and Control* (DISCC), responsable de la direction opérationnelle du travail de renseignement et qui est placé sous les ordres du Chef du SGRS. Une autre section importante du DISCC est le *Collection Coordination Intelligence Requirements Management* (CCIRM), qui joue un rôle crucial dans la coordination et le traitement de toutes les informations entrantes (*Requests for Information* (RFI), rapports HUMINT) et sortantes (*Requests for Collect* (RFC), notes aux autorités).

---

104 En 2018, la VSSE a communiqué les informations dont elle disposait sur Jürgen Conings lors d'une réunion du Groupe de travail Extrême droite (Plan R). Le SGRS n'a pas non plus répondu formellement à une note du 8 janvier 2021, dans laquelle la VSSE faisait part de ses préoccupations concernant Jürgen Conings. Le SGRS aurait toutefois évoqué la question lors d'une réunion bilérale qui a eu lieu le 15 janvier 2021.

105 Voir à ce propos *in extenso* le rapport commun des Comités permanents R et P ('I.10 Enquête commune de contrôle sur le rôle de l'OCAM dans le suivi du militaire Jürgen Conings'). Les collaborateurs du SGRS soulignent que le niveau 3 de la menace n'a pas été transmis au SGRS dans une évaluation de la menace distincte de l'OCAM. L'OCAM fait cependant remarquer que les évaluations de la menace portant sur des personnes mentionnées dans la BDC TF ne peuvent être consultées que via ce canal.

Plusieurs collaborateurs expriment leurs doutes sur la connaissance du fonctionnement du service et de l'expérience en matière de travail de renseignement des collaborateurs qui font partie du DISCC (plus particulièrement le CCIRM). Ce manque de connaissances et d'expérience expliquerait l'orientation souvent lente et erronée des informations. Les doutes que nourrissent certains collaborateurs sur son bon fonctionnement font que les informations circulent en dehors du DISCC, d'où l'apparition de flux d'informations parallèles.

Dans ce dossier, les collaborateurs de la plateforme d'analyse PF6 ont expliqué qu'une note importante de la VSSE de janvier 2021, dans laquelle ce service se dit préoccupé par Jürgen Conings et pose une série de questions au SGRS, n'est jamais parvenue à la PF6, et est dès lors restée sans réponse. Selon la PF6, le DISCC n'a pas introduit la note en question dans le système *Request for Information Management*, normalement utilisé pour les questions entrantes des services externes.

Au sein du DISCC, les membres du *Steering Comittee*, censés prendre des décisions opérationnelles, ne sont pas suffisamment informés du contenu des dossiers. Ces décisions sont en outre rarement consignées officiellement, ce qui génère de la confusion.

Une troisième section essentielle du DISCC est constituée par ce que l'on appelle les *Case Managers* (CaMa) et les *Collection Managers* (CoMa), chargés de traduire les besoins en informations des plateformes d'analyse dans la mise en oeuvre de moyens de collecte, lorsqu'il faut recourir aux méthodes particulières de renseignement/méthodes de recueil de données (MRD). Toutefois, les CaMa et CoMa ne relèvent pas des mêmes structures (Directions) que les plateformes d'analyse et les services de collecte. Ces Directions ont quant à elles leur propre structure et leur propre hiérarchie, ce qui donne lieu à des controverses sur les compétences et les priorités. Par exemple, dans la structure actuelle, le chef de la section C6/Investigations (qui fait partie de la Direction Collecte) n'est pas compétent pour décider de l'affectation de ses collaborateurs.

L'enquête a également démontré la trop faible valorisation des détachements provinciaux[106], impliqués dans les LTF et en contact avec les commandants de corps et les officiers de sécurité des unités. Le Comité constate que cette 'proximité' est trop peu utilisée par les services centraux d'Evere. Plus précisément, les détachements provinciaux sont trop peu guidés.[107]

En outre, il est apparu qu'il y a peu de concertation entre les détachements provinciaux et le quartier général, ce qui fait que les collaborateurs dans les détachements provinciaux se sentent quelque peu abandonnés à leur sort et doivent

---

106 Les détachements provinciaux constituent une sorte d'antenne du SGRS dans chacune des provinces et sont donc plus proches des unités militaires que des services centraux à Evere. Leur position leur permet donc de détecter rapidement certains développements ou de suivre de près certaines affaires/événements. Mais ils sont aussi souvent les mieux placés pour répondre aux questions des service centraux, étant donné qu'ils ont des contacts sur place et connaissent l'environnement.

107 Le Comité permanent R avait déjà attiré l'attention sur ce point-là aussi à plusieurs reprises.

établir eux-mêmes leurs priorités. Il n'y a ainsi eu aucune concertation à propos de l'inscription de Conings dans la BDC TF entre la plateforme d'analyse compétente et le collaborateur du détachement provincial du Limbourg, qui représentait le SGRS à la LTF compétente.

C'est le détachement du Limbourg qui, en novembre 2019, a fait mention de Jürgen Conings pour la première fois, notamment son implication dans le groupement d'extrême droite *Belgian Commandery of Knights Templar*. Ensuite, jusque fin juin 2020, moment où le détachement provincial informe à nouveau les services centraux qu'il a été contacté par la Police fédérale et le parquet parce que l'intéressé recherchait l'adresse de Marc Van Ranst via Facebook, il n'y a eu pas eu d'autres communications entre les services centraux à Evere et le détachement provincial. Il n'a pas été demandé au détachement de recueillir des informations supplémentaires.

I.9.3.4. La 'watchlist' extrême droite

La ministre de la Défense a demandé au Comité permanent R d'évaluer la 'fiabilité' de la 'watchlist' établie par le SGRS. Dans le cadre de son enquête, le Comité a pu constater que la 'watchlist' constituait un processus interne au SGRS. Retravaillée à la suite de précédentes recommandations du Comité permanent R[108], une nouvelle 'watchlist' a été réalisée en avril 2021 et rassemble les fiches individuelles relatives aux personnes apparaissant dans le suivi de la menace extrême droite par le SGRS.

Ce processus a pour finalité de déterminer, sur la base d'une réévaluation périodique, les niveaux des menaces individuelles relevant de l'extrême droite et le suivi qu'il convient d'y donner (collecte additionnelle d'informations, échange d'informations avec d'autres services, identification de mesures curatives, retrait de la personne concernée de la 'watchlist' lorsqu'il s'avère qu'elle ne constitue pas/plus une menace, etc.).

Par conséquent, la 'watchlist' ne constitue pas un recueil exhaustif des données au sujet des personnes apparaissant dans le périmètre de la menace liée à l'extrémisme de droite et relevant de la compétence du SGRS. Elle doit être combinée avec d'autres informations. Aussi, en tant que processus interne, elle n'a pas vocation à être communiquée comme telle à des tiers au SGRS. Le concept de 'fiabilité' au regard duquel la ministre de la Défense a demandé d'évaluer la 'watchlist' n'étant pas consacré en tant que tel dans les règles régissant les activités du SGRS, le Comité permanent R a décidé d'évaluer les données (à caractère personnel) reprises dans la 'watchlist' au regard du standard juridique de qualité des données traitées prescrit dans les articles 75, 3° et 4°, et 83, 1° de la Loi sur la protection des données. En effet, plus les données traitées sont adéquates,

[108] Voir COMITÉ PERMANENT R, *Rapport d'activités 2020,* 169-171 ('Diverses recommandations relatives à l'enquête de contrôle sur le suivi de l'extrême droite').

pertinentes, non excessives, complètes et mises à jour *en fonction de la finalité* de la 'watchlist', plus cette dernière peut être considérée comme 'fiable'.

Dans ce cadre normatif, compte tenu de la finalité de la 'watchlist', à savoir un processus de travail interne, en cours d'élaboration, d'identification et de suivi de la menace émanant de l'extrême droite relevant de la compétence du SGRS, le Comité a considéré que la conformité de la 'watchlist' aux articles 75, 3° et 4°, et 83, 1° LPD n'appellait pas de commentaire particulier. Le Comité permanent R a toutefois estimé nécessaire d'émettre une série de recommandations à l'égard du SGRS, en vue de poursuivre, finaliser et documenter le processus de travail que constitue la 'watchlist'.

I.9.3.5. Les habilitations de sécurité successives de Jürgen Conings

Jürgen Conings était titulaire d'une habilitation de sécurité de niveau SECRET[109] depuis le 21 août 2006. Cette habilitation avait depuis fait l'objet de multiples renouvellements malgré l'existence de notices de police à propos de l'intéressé (concernant des faits de menaces et de coups et blessures).

Lors de la procédure de renouvellement initiée par son officier de sécurité en 2019, la VSSE signale un « *hit* » et, dans un document interne, rend notamment compte de deux faits à caractère judiciaire dont un concernant la détention illégale d'armes. Contactée par le SGRS, la VSSE transmet ces informations, d'abord oralement puis par voie électronique, mentionnant que Jürgen Conings est connu pour l'appartenance à un groupe Facebook défendant les intérêts assyriens en Irak. Les faits de 2015 sont mentionnés, mais pas ceux de 2018. Sur base de ces informations, le SGRS lance une première analyse SOCMINT. Celle-ci révèle des liens potentiels avec des mouvances d'extrême droite. À la suite d'une interview avec l'intéressé, les enquêteurs du SGRS concluent que les faits détectés en relation avec l'extrême droite ne sont pas de nature à nuire à son habilitation de sécurité, mais préconisent quand même une mise en garde.

Le 24 juin 2020, Conings obtient le renouvellement de son habilitation. Deux jours plus tard, alors que des menaces sont proférées à l'encontre de Marc Van Ranst, un analyste du SGRS identifie Jürgen Conings sur les vidéos de surveillance et un rapport administratif (RAR) de la police complète le tableau. Une deuxième analyse SOCMINT est diligentée et révèle de nouveaux liens plus inquiétants avec l'extrême droite. Sur la base de ces éléments, le SGRS refuse le renouvellement de l'habilitation de sécurité le 31 août 2020.[110]

---

109 Dans son article 4, la L.C&HS distingue trois degrés de classification : CONFIDENTIEL, SECRET, TRÈS SECRET.

110 Vu les délais, Jürgen Conings n'était plus habilité dès le 17 juillet 2020. Pour rappel, cette absence ou ce refus n'avait aucune conséquence sur sa nouvelle fonction au sein de la Défense.

I.9.3.6. La mission d'officier de sécurité

Le 2 juin 2020, Jürgens Conings a fait mutation vers sa nouvelle unité (PDT-IA) dans une fonction ne nécessitant plus d'habilitation de sécurité. L'officier de sécurité en charge de sa nouvelle unité n'a pas mis fin à la demande de renouvellement. En effet, dans certains cas de figure et dans le cadre de déploiements, une telle habilitation est nécessaire.

Début septembre 2020, l'officier de sécurité a été informé par le SGRS du non-renouvellement. Vu les circonstances liées au COVID, il a informé par téléphone l'intéressé dudit refus. La notification verbale a été confirmée par écrit le 12 novembre 2020 soit 2 mois et demi après le refus.

Au sein du SGRS, le Règlement IF5 décrit les responsabilités de l'officier de sécurité, en charge notamment de l'élaboration d'ordres permanents de sécurité et du contrôle de leur application. Aucune mention n'est toutefois faite de la collaboration et des interactions avec le personnel du SGRS.

Le cas de l'officier de sécurité de Jürgen Conings est particulier. Responsable d'une multitude de petites entités indépendantes, il est délocalisé par rapport aux unités qu'il doit contrôler. Cette délocalisation ne lui permet certainement pas un contrôle effectif de l'application des directives de sécurité.

Le Comité permanent R a en outre constaté que le SGRS n'avait pas communiqué avec l'officier de sécurité de l'unité de Jürgen Conings dans le cadre du refus de son habilitation. Le Comité a également constaté que l'officier de sécurité était dans l'incapacité d'exercer un contrôle sur l'ensemble des unités dont il a la charge.

I.9.3.7. Le dépôt d'armes et le rôle du SGRS

Le 18 mai 2021, un collègue de Jürgen Conings constate que des armes et des munitions sont manquantes dans l'armurerie et le dépôt de munitions dédiés à la Cellule PDT-IA. Il signale immédiatement l'incident à sa hiérarchie et déclenche une enquête interne au niveau de la Direction S du SGRS. Les directives internes du SGRS (en particulier le règlement IF5(bis)) excluent pourtant qu'un même individu puisse être à la fois gestionnaire d'armes et de munitions. Le Règlement IF5 attribue également un statut spécial à ces locaux. Ainsi, les gestionnaires des dépôts de munitions et d'armurerie devraient disposer d'une habilitation de sécurité. L'enquête a révélé que ces règles n'étaient pas respectées au sein de la Cellule PDT-IA. La multiplication d'adaptations aux règles, couplée aux aménagements liés à l'épidémie de Covid-19, ont permis à Jürgen Conings d'avoir accès à l'arsenal avec lequel il a pris la fuite.

I.9.4. CONCLUSIONS

L'affaire Conings est une illustration des manquements constatés par le Comité permanent R ces dix dernières années au sein des services de renseignement et de sécurité en général, et au sein du service de renseignement militaire en particulier. Avec l'affaire Conings, on ne peut pas nier que c'est le service de renseignement militaire qui se retrouve dans la tourmente. Il est indéniable que des erreurs (graves) ont été commises à tous les niveaux du SGRS, mais aussi dans toute la ligne hiérarchique de la Défense : un manque d'effectifs structurel dans les différents services et à tous les niveaux, une grande rotation du personnel, la perte de connaissances et d'expérience, une supervision limitée dans l'unité de Conings, une défaillance manifeste dans le flux d'informations (*bottom up* et *top down*), une nouvelle structure de travail complexe au SGRS, trop peu d'orientation, des problèmes relatifs au personnel, aucune politique claire en matière d'extrémisme, un échange d'informations défaillant au sein de la Défense et entre les différents acteurs de la sécurité, etc. Des erreurs ont peut-être aussi pu être constatées dans le chef d'autres acteurs (police, parquets, juges d'instruction, etc.). L'examen de ces éventuelles erreurs sort du domaine de compétence du Comité permanent R.

Il a pu être constaté que les faits dans cette affaire ont été détectés à temps par les services de renseignement et de sécurité, mais ils n'ont pas fait l'objet d'un suivi suffisamment actif. La marge d'amélioration est importante.

Il est indéniable, pour le Comité permanent R, que le SGRS est nécessaire, voire indispensable, dans l'architecture générale de la sécurité tant en Belgique qu'à l'étranger. Son fonctionnement doit néanmoins être modifié en profondeur. Et sa structure tout autant. L'idéal serait de réduire ses tâches au minimum afin de lui permettre de se régénérer calmement et d'aboutir au *change management* attendu dans le cadre d'une professionnalisation mise au service de la sécurité du citoyen.

I.10. ENQUÊTE COMMUNE DE CONTRÔLE SUR LE RÔLE DE L'OCAM DANS LE SUIVI DU MILITAIRE JÜRGEN CONINGS

En complément de l'enquête de contrôle concernant le suivi de Jürgen Conings par les deux services de renseignement[111], le Comité permanent R a également examiné, conjointement avec le Comité permanent P, « *le rôle de l'OCAM dans le suivi de Jürgen Conings, à savoir en ce qui concerne l'enquête préliminaire, l'évaluation de la menace de niveau 3 et ses conséquences et l'échange d'informations à propos de l'intéressé* ». Les Comités permanents R et P se sont ainsi intéressés à la

[111] Voir 'I.9. Enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings'.

position d'information de l'OCAM, au processus d'évaluation de la menace posée par l'intéressé ainsi qu'à l'échange d'informations entre les partenaires.[112]

I.10.1. ANALYSE DU CADRE LÉGAL

La Loi relative à l'analyse de la menace du 10 juillet 2006 (L.OCAM) confie à l'OCAM la mission d'effectuer ponctuellement une évaluation commune des éventuelles menaces en matière de terrorisme et d'extrémisme et, le cas échéant, les mesures qui s'avèrent nécessaires.

Pour évaluer la menace, l'OCAM se base sur les renseignements provenant de ses services d'appui (par exemple, la VSSE, le SGRS et la Police fédérale). Selon la L.OCAM, les services d'appui sont tenus (sous peine d'une sanction pénale), sauf en cas de procédure d'embargo, de communiquer à l'OCAM, d'office ou à la demande de son directeur, tous les renseignements dont ils disposent dans le cadre de leurs missions légales et qui s'avèrent pertinents pour l'accomplissement des missions de l'OCAM dans les délais prévus par l'Arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace. Le flux d'informations entre l'OCAM et ses services d'appui varie selon qu'il s'agisse de documents classifiés ou non. Les informations classifiées sont échangées par BINII et ensuite enregistrées par l'OCAM dans sa base de données PROTEUS. La messagerie fonctionnelle de l'OCAM est utilisée pour tout l'échange d'informations non classifiées.

L'article 11 §6 de l'arrêté d'exécution de la L.OCAM stipule que chaque évaluation déterminera le niveau de la menace en s'appuyant sur une description de la gravité et de la vraisemblance du danger ou de la menace.[113] Selon l'article 10 L.OCAM, les évaluations ponctuelles de la menace concernant des personnes, des groupements, des objets ou des événements, exécutées d'initiative par l'OCAM, sont communiquées aux membres du Conseil national de sécurité, aux services d'appui, à la Direction générale du Centre de crise, au Parquet fédéral et au membre du Collège des procureurs généraux à qui est confiée la matière du terrorisme et de l'extrémisme, à l'Autorité nationale de sécurité (ANS) ainsi qu'à tout membre du gouvernement que le directeur de l'OCAM juge nécessaire d'informer.

---

112 Jusqu'au 17 mai 2021, jour de la disparition de Jürgen Conings.

113 Les différents niveaux de la menace sont :
- le « Niveau 1 ou FAIBLE » lorsqu'il apparaît que la personne, le groupement ou l'événement qui fait l'objet de l'analyse n'est pas menacé ;
- le « Niveau 2 ou MOYEN » lorsqu'il apparaît que la menace à l'égard de la personne, du groupement, ou de l'événement qui fait l'objet de l'analyse est peu vraisemblable ;
- le « Niveau 3 ou GRAVE » lorsqu'il apparaît que la menace à l'égard de la personne, du groupement ou de l'événement qui fait l'objet de l'analyse est possible et vraisemblable ;
- le « Niveau 4 ou TRES GRAVE » lorsqu'il apparaît que la menace à l'égard de la personne, du groupement ou de l'événement qui fait l'objet de l'analyse est sérieuse et imminente.

L'évaluation de la menace que représente une personne est quant à elle régie par l'Arrêté royal relatif à la banque de données commune *Foreign Terrorist Fighters* du 21 juillet 2016 (AR BDC) et la circulaire du 22 mai 2018 du ministre de la Sécurité et de l'Intérieur et du ministre de la Justice relative à l'échange d'informations et au suivi des *Terrorist Fighters* et des Propagandistes de haine (diffusion restreinte) (CM BDC). Dans le cadre de cette enquête, les Comités permanents R et P se sont penchés plus spécifiquement sur la création et l'alimentation de la banque de données commune *Terrorist Fighters* (BDC TF).

I.10.2. L'OCAM ET LES BANQUES DE DONNÉES COMMUNES

Après les attentats de 2016, la Loi du 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme a modifié la Loi du 5 août 1992 sur la fonction de police (LFP) et prévoit une base légale pour la constitution d'une banque de données commune afin de renforcer la prévention et la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme.

L'AR BDC a ensuite effectivement créé la banque de données commune *Foreign Terrorist Fighters*. Par un arrêté de modification du 23 avril 2018, cette banque de données a été rebaptisée banque de données commune *Terrorist Fighters* (BDC TF) en raison de l'ajout d'une nouvelle catégorie *Homegrown Terrorist Fighters* à côté de la catégorie *Foreign Terrorist Fighters* existante. Un nouvel arrêté royal à la même date a créé une banque de données commune distincte pour les Propagandistes de haine (BDC PH).[114]

Enfin, l'arrêté royal du 20 décembre 2019 a ajouté deux nouvelles catégories à la banque de données commune *Terrorist Fighters*, à savoir les Extrémistes Potentiellement Violents et les Personnes condamnées pour terrorisme.[115] En application de l'AR FTF et des AR de modification de 2018 et 2019, la BDC TF organise donc désormais le suivi des *Foreign Terrorist Fighters* (FTF), des *Homegrown Terrorist Fighters* (HTF), des Extrémistes Potentiellement Violents (EPV) et des Personnes condamnées pour terrorisme (PCT).

Afin de renforcer l'échange d'informations, la loi prévoit une obligation d'alimentation de la BDC pour les services ayant un accès direct aux banques de données communes. Les données relatives à une entité enregistrée dans la BDC

---

114 Arrêté royal 23 avril 2018 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters portant exécution de certaines dispositions de la section 1 er*bis* « de la gestion des informations » du chapitre IV de la loi sur la fonction de police et modifiant la banque de données commune Foreign Terrorist Fighters vers la banque de données commune Terrorist Fighters, et A.R. du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1er*bis* « de la gestion des informations » du chapitre IV de la loi sur la fonction de police, *M.B.*, 30 mai 2018.

115 A.R. du 20 décembre 2019 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters, *M.B.* 27 janvier 2020.

doivent ainsi continuellement être tenues à jour. C'est en ce sens que la BDC est une banque de données dynamique. Seuls les services de base (OCAM, VSSE, SGRS et police intégrée) peuvent créer une nouvelle entité dans la BDC et, après validation de l'OCAM, placer une personne en pré-enquête pour une durée de 6 mois maximum. Pour chaque entité enregistrée, les services avec accès direct à la BDC veillent à ajouter les données à caractère personnel et informations dont ils disposent. Chaque service ne peut modifier ou supprimer que les données et informations qu'il a lui-même enregistrées.

En tant que responsable opérationnel de la BDC, l'OCAM est chargé de l'évaluation des informations de la fiche de renseignements (voir *infra*) et de la validation d'une entité dans la BDC sur la base des informations fournies par les partenaires.

I.10.2.1. La procédure d'inscription

La procédure d'inscription pour la catégorie d'EVP – catégorie introduite par l'AR du 20 décembre 2019 et dans laquelle Jürgen Conings était repris – est développée dans la circulaire du ministre de l'Intérieur et de la Sécurité et du ministre de la Justice du 22 mai 2018 relative à l'échange d'informations et au suivi des TF et des PH (CM BDC).[116] Cette circulaire décrit en réalité l'échange d'informations concernant les catégories FTF, HTF et PH, mais elle est appliquée, par analogie, aux EPV[117].

La phase de « pré-enquête » (dite « phase d'enrichissement ») vise la phase de collecte de données et d'informations, à charge et à décharge, nécessaires à la

---

116 L'objectif général de la circulaire est : « *partant d'un objectif de sécurité, régler la gestion de l'information, la prise de mesures et la collaboration coordonnée entre les services concernés dans le but de garantir la protection maximale de la sécurité publique face à la menace potentielle et de contrecarrer la menace émanant des Terrorist Fighters (FTF/HTF) et des propagandistes de haine.* »

117 La catégorie EPV concerne toute personne physique ayant un lien avec la Belgique et qui répond aux critères cumulatifs suivants :

a) cette personne a des conceptions extrémistes qui justifient l'usage de la violence ou de la contrainte comme méthode d'action en Belgique ;

b) il existe des indications fiables qu'elle a l'intention de recourir à la violence, et ce en relation avec les conceptions mentionnées en a) ;

c) l'EPV répond au minimum à une des conditions suivantes quant au risque de violence : 1) il entretient systématiquement des contacts sociaux au sein de milieux extrémistes ; 2) il a des problèmes psychiques constatés par un professionnel compétent en la matière ; 3) il a commis des actes ou présente des antécédents qui peuvent être considérés comme soit a) un crime ou un délit portant atteinte à ou menaçant l'intégrité physique ou psychique de tiers ; soit b) des instructions ou des formations relatives à la fabrication ou l'utilisation d'explosifs, d'armes à feu ou d'autres armes ou substances nocives ou dangereuses, ou pour d'autres méthodes et techniques spécifiques en vue de commettre des infractions terroristes conformément à l'article 137 du Code pénal ; soit c) des agissements en connaissance de cause constituant un soutien matériel en faveur d'une organisation ou d'un réseau terroriste/extrémiste ; soit d) des agissements dont la nature indique un niveau de vigilance préoccupant de l'individu à l'égard de la sécurité.

validation ou non d'une entité en tant qu'EPV. La CM BDC encourage les services à déterminer ensemble, au sein des LTF et dans le respect de leurs missions légales respectives, la stratégie de récolte d'informations afin d'enrichir les renseignements ('qui fait quoi'). À l'issue de cette période de maximum six mois, sur la base des informations et renseignements disponibles, l'OCAM évalue si les critères légaux sont rencontrés. Si ce n'est pas le cas, les données de la personne en pré-enquête sont automatiquement effacées.

Conformément à ce que prévoit la CM BDC, la BDC se compose de fiches de renseignements reprenant les données à caractère personnel et les informations non classifiées qui proviennent de tous les services qui alimentent la BDC. Ces fiches permettent non seulement d'évaluer la menace que représentent les entités mais surtout d'en assurer le suivi afin d'anticiper et d'empêcher de potentielles infractions terroristes.

Lorsque le statut dans la BDC est validé, l'OCAM procède à une évaluation de la menace individuelle à partir des informations pertinentes dont il dispose. Cette évaluation, intégrée dans la fiche de renseignements individuelle, permet d'orienter les mesures de suivi prises par les partenaires.

Afin d'évaluer les critères d'attribution d'un statut et le niveau de la menace, l'OCAM s'appuie sur son propre outil d'évaluation du risque, RooT37. À l'aide d'indicateurs inspirés de la littérature scientifique, l'outil définit un score indicatif. Ce score est ensuite contrôlé par un évaluateur de l'OCAM, puis, une nouvelle fois, par une « équipe qualité » avant d'être définitivement validé.

I.10.2.2. L'échange d'informations avec les partenaires

Dans le cadre du Plan R[118], l'échange d'informations est notamment organisé au sein des LTF qui sont des plateformes de concertation opérationnelles et stratégiques, destinées aux services de police et de renseignement et installées dans chaque arrondissement judiciaire,[119] et des cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme (CSIL-R), qui sont des plateformes de concertation communales chargées de la réalisation d'actions préventives, répressives et de suivi cohérentes. Comme les LTF, elles sont des plateformes de concertation, théâtre d'échange d'informations entre les services de prévention et sociaux, la LTF et les autorités administratives concernant le radicalisme, l'extrémisme et le terrorisme.

Conformément à la CM BDC, les LTF jouent un rôle crucial dans la définition des mesures de sécurité. Ainsi, lors des réunions des LTF, les partenaires s'accordent

118 Devenu 'Stratégie Extrémisme et Terrorisme' (Stratégie TER) en septembre 2021.

119 Elles ont pour but de garantir le suivi au niveau local d'individus et de groupements radicalisants ainsi que de réduire leur impact en proposant des mesures en échangeant et discutant notamment d'informations, de renseignements et d'analyses.

sur la priorisation des entités à suivre selon la menace qu'elles représentent et sur leur degré de coopération avec les autorités.

I.10.3. LE RÔLE DE L'OCAM DANS LE SUIVI DE JÜRGEN CONINGS : L'INSCRIPTION DANS LA BANQUE DE DONNÉES COMMUNE

En août 2020, l'OCAM a ouvert une pré-enquête EPV concernant Jürgen Conings. Cette décision repose sur l'analyse des informations transmises par la police et les services de renseignement dès juin 2020. L'OCAM a également procédé à une analyse de son activité sur les réseaux sociaux. Encodées dans la banque de données de l'OCAM, PROTEUS, ces informations concernaient notamment les menaces proférées par l'intéressé et ses contacts au sein des milieux d'extrême droite. Au regard des informations disponibles, les Comités permanents R et P estiment la décision de pré-enquête justifiée.

Dès l'ouverture d'une pré-enquête, les services de base ont l'obligation d'enrichir la BDC de toutes les informations pertinentes dont ils disposent. Le suivi doit en outre être assuré au sein de la LTF compétente. L'analyse des PV des réunions de la LTF et du groupe de travail Extrême droite (Plan R) confirme l'inscription du suivi de Jürgen Conings à l'ordre du jour dès septembre 2020.

À la fin de la pré-enquête et à l'aide de son outil Root37, l'OCAM a réalisé une évaluation des éléments dont il disposait au regard des critères de validation définis dans l'AR BDC. Le statut d'EPV a été confirmé et la menace présentée par Jürgen Conings a été évaluée au niveau 3 (grave). Cette évaluation a été confirmée par l'évaluateur de l'OCAM et l'équipe qualité à la mi-février 2021.

I.10.4. L'ÉCHANGE D'INFORMATIONS

L'OCAM a informé les différents partenaires de la LTF concernée de l'inscription de Jürgen Conings dans la BDC et de l'évaluation de la menace lors d'une réunion fin février 2021 à laquelle le SGRS n'a pas participé. Le procès-verbal de la réunion rend compte des échanges à propos de l'intéressé.

L'enregistrement de Jürgen Conings dans la BDC a en outre été communiqué à la Police fédérale (pour signalement dans la Banque de données nationale générale ou BNG), à BELPIU ainsi qu'à la CSIL-R pertinente (et donc au bourgmestre). L'OCAM n'a toutefois envoyé aucune alerte supplémentaire aux services de base et à ses partenaires concernant l'évaluation de niveau 3 de l'intéressé, estimant suffisante l'inscription dans la BDC.

Après son inscription dans la BDC, le suivi de Jürgen Conings figurait à l'ordre du jour de chaque réunion de la LTF et du groupe de travail Extrême droite, bien

que de nouvelles informations n'aient pas toujours été disponibles (voir *infra*). L'unique information complémentaire transmise à l'OCAM avant le 17 mai 2021 n'a pas justifié de modification du niveau de la menace.

L'inscription en tant qu'EPV/niveau 3 dans la BDC permet en outre l'échange d'informations avec les services ayant uniquement un accès *hit/no hit* qui, lors de la consultation de la BDC, sont également informés qu'une personne est connue. Dans le cas de Jürgen Conings, la Direction générale Sécurité & Prévention du SPF Intérieur a par exemple consulté la BDC (et obtenu un « *hit* ») dans le cadre de la demande par l'intéressé d'une carte d'identification d'agent de gardiennage.

Conformément à la CM BDC, chaque personne inscrite dans la BDC se voit attribuer une catégorie (A, B ou C) dans le cadre du suivi en LTF. Lors de son inscription, Jürgen Conings a été classé en catégorie B, à savoir une « menace pas particulièrement élevée ». Les Comités permanents R et P ont pointé le manque de cohérence entre le niveau de menace défini par l'OCAM (3 soit grave), d'une part, et la catégorie pour le suivi en LTF, d'autre part. L'OCAM précise que les mesures de suivi sont semblables pour les catégories A, B et C mais relève, plus généralement, la difficile application des mesures prévues dans la CM BDC qui reste non contraignante.[120]

En ce qui concerne les autres mesures, comme le « suivi proactif », l'OCAM constate que même avec les FTF, il n'est pas toujours évident d'y parvenir, étant donné que ceci n'est pas exécutoire et que la CM BDC se heurte à ses limites au niveau des mesures. Si aucune information ou enquête pénale pour terrorisme ne peut être ouverte, pas grand-chose n'est alors possible. Dans le cas de Jürgen Conings, une enquête judiciaire était en cours pour les menaces à l'encontre de Marc Van Ranst.[121] L'OCAM constate qu'en dehors de ce qui a été communiqué au sein de la LTF, il n'a reçu aucune autre information à propos de l'enquête judiciaire en cours.

Une autre conséquence du statut EPV de niveau 3 est qu'il devrait être abordé au sein de chaque LTF pour déterminer quelles informations émergent et identifier éventuellement les mesures à adopter pour réduire la menace. Aux yeux de l'OCAM, l'initiative incombe au SGRS, étant donné qu'il s'agissait d'un militaire. Néanmoins, la récolte d'informations est attendue de tous les services. Lors des réunions de la LTF de mars et d'avril 2021, l'intéressé figurait à l'ordre du jour mais n'a été abordé par aucun service, et aucune information à ce sujet n'a dès lors été partagée.

En application de la note 'Signalements' élaborée par DJSOC/Terro (Direction de la lutte contre la criminalité grave et organisée (section terrorisme) de la Police judiciaire fédérale), chaque EPV est signalé dans la BNG pour un « contrôle discret ». Selon l'OCAM, cette mesure n'a pas permis de récolter davantage

120 Pour l'OCAM, l'octroi de cette catégorie B ne veut pas dire qu'il est procédé à une évaluation supplémentaire. La catégorie B doit en effet également être suivie de près.

121

d'informations. Dans le cas contraire, ces informations auraient été abordées au sein d'une LTF.

I.10.5. CONCLUSIONS

L'enquête des Comités permanents R et P relative au rôle de l'OCAM dans le suivi de Jürgen Conings confirme le partage d'informations à l'OCAM par les services de base lors de la phase de pré-enquête dès août 2020. Sur la base de ces informations enregistrées dans PROTEUS et à l'aide de l'outil Root37, le statut EPV de Jürgen Conings a été validé et le niveau de menace évalué à 3.

C'est l'OCAM qui a pris l'initiative de placer Jürgen Conings en pré-enquête EPV et de lui attribuer le statut d'EPV de niveau 3. Les Comités permanents R et P ont estimé la décision de pré-enquête justifiée.

L'évaluation de la menace posée par Jürgen Conings a été communiquée par l'OCAM selon les modalités prévues par la L.OCAM. Evalué au niveau 3 de menace (grave), Jürgen Conings n'a par contre été placé qu'en catégorie B (menace pas particulièrement grande) dans le cadre du suivi en LTF. Les deux paramètres sont en effet indépendants.

I.11. LE SUIVI D'UN COMMISSAIRE DU GOUVERNEMENT PAR LA VSSE

Par arrêté royal du 17 mai 2021, Ihsane Haouach a été nommée comme commissaire du gouvernement auprès de l'Institut pour l'égalité entre les femmes et les hommes (IEFH). En cette qualité, elle représentait le gouvernement au conseil d'administration de l'IEFH. Elle a cependant été sous le feu des critiques dès sa nomination : d'une part en raison de son voile, et d'autre part, en raison des propos qu'elle a tenus sur la séparation entre l'Église et l'État. Le 9 juillet 2021, Ihsane Haouach a présenté sa démission. Le même jour, il a été suggéré dans les médias qu'une note de la Sûreté de l'État (VSSE) pourrait en être à l'origine.[122]

[122] B. DEMONTY, *Le Soir*, 9 juillet 2021 ('Ihsane Haouach démissionne, le gouvernement en possession d'informations sur de potentiels liens avec les Frères musulmans'). Le rapport de la VSSE en question ('Diffusion restreinte'/ 'Confidentiel') est également paru intégralement dans la presse (par ex. M. VERBERGT, *De Standaard*, 14 juillet 2021 ('Dit zegt de Staatsveiligheid letterlijk over Ihsane Haouach')).

I.11.1. UNE NOTE DE LA SÛRETÉ DE L'ÉTAT

Courant 2020, la Section d'Analyse Contre-extrémisme (CE) de la VSSE a rédigé une note de synthèse sur les Frères musulmans en Belgique.[123] Au moment où la controverse est née dans la presse autour de la nomination de Ihsane Haouach comme commissaire du gouvernement, on se souvient à la VSSE que son nom était apparu dans cette note de synthèse. L'intéressée n'était cependant pas une 'cible' du service. En revanche, la VSSE suit des agissements dans le cadre de la lutte contre diverses formes d'extrémisme, ce qui s'inscrit dans ses missions légales (art. 8 L.R&S, 'extrémisme').

La VSSE a jugé opportun d'informer par écrit le ministre de la Justice et le Premier ministre à ce propos. Une note classifiée a été rédigée à cet effet. Il semblait qu'Ihsane Haouach était *'gekend omwille van haar nauwe contacten met de Moslimbroeders. Deze contacten tussen de Moslimbroeders en Ihsane Haouach kunnen worden gekaderd binnen een bredere strategie van de Moslimbroeders, waarbij deze proberen te wegen op het publieke debat en de beleidsvorming […]'*.[124] Il était également mentionné que l'intéressée *'voor zover ons bekend zelf geen lid is van de Moslimbroeders en zelf nooit de aandacht heeft getrokken omwille van concrete extremistische stellingnames' […] Het is dan ook niet uit te sluiten dat Ihsane Haouach er zich zelf niet (ten volle) van bewust is dat ze nauwe contacten onderhoudt met de Moslimbroeders. We stellen dan ook voor om de bevoegde Staatssecretaris of haar Beleidscel, net als eventueel mevrouw Haouach zelf, een sensibiliserende briefing aan te bieden*'.[125] [126]

---

123 Voir à ce propos 'I.12. Une attention renouvelée pour les Frères musulmans' (*infra*).

124 *'connue en raison de contacts étroits avec les Frères musulmans. Ces contacts entre les Frères musulmans et Ihsane Haouach peuvent s'inscrire dans une stratégie plus large des Frères musulmans, par laquelle ils tentent d'influencer le débat public et l'élaboration de politiques […]'* (traduction libre).

125 *'du moins à notre connaissance, n'est elle-même pas membre des Frères musulmans et n'a jamais attiré l'attention en raison de positions extrémistes concrètes […]. Il ne peut donc être exclu que Ihsane Haouach elle-même ne soit pas (pleinement) consciente du fait qu'elle a des contacts étroits avec les Frères musulmans. Nous suggérons dès lors de briefer la Secrétaire d'État compétente et sa Cellule stratégique, mais éventuellement aussi Madame Haouach elle-même, et ce afin de les sensibiliser à cette problématique.'* (traduction libre).

126 Citation reprise de la note confidentielle de la VSSE qui a été publiée dans la presse (M. VERBERGT, *De Standaard*, 14 juillet 2021 ('Dit zegt de Staatsveiligheid letterlijk over Ihsane Haouach')).

I.11.2. CONSTATATIONS DE L'ENQUÊTE

I.11.2.1. Une attention renouvelée pour les Frères musulmans (et Ihsane Haouach) ?

Si la lutte contre le terrorisme continue de figurer en haut de la liste de ses priorités, la VSSE a de nouveau porté son attention sur d'autres dossiers au cours de ces dernières années. Dans le cadre des menaces 'extrémisme' et 'ingérence', il a été décidé en 2020 de rédiger une note de synthèse sur les Frères musulmans en Belgique, qui constitue une des priorités de la VSSE dans son Plan d'action. Le nom de Ihsane Haouach est apparu dans le contexte de cette note, comme étant une personne qui, consciemment ou non, était en contact avec cette mouvance. L'intéressée n'était cependant pas une 'cible' de la VSSE.

Par le biais de (l'agitation dans) la presse, la VSSE apprenait la nomination de Ihsane Haouach comme commissaire du gouvernement. Le service prit l'initiative de rédiger une note, estimant qu'il convenait en premier lieu d'informer le ministre de la Justice du fait que l'intéressée était connue dans le cadre du suivi des compétences légales en matière d'extrémisme. Étant donné qu'il n'était exclu que l'intéressée elle-même ne soit pas (pleinement) consciente d'entretenir des liens étroits avec les Frères musulmans, il était proposé au ministre d'organiser un briefing de sensibilisation pour la Secrétaire d'État ou sa Cellule stratégique, y compris pour Ihsane Haouach dans une phase ultérieure.

I.11.2.2. Le principe de précaution

Dans un contexte de renseignement, il n'y a que peu de certitudes, ce qu'il faut garder à l'esprit quand il s'agit de décider de communiquer des informations et de la manière de les communiquer (dans le cas présent, au ministre de la Justice). Le Comité avait précédemment affirmé que « *(p)our pouvoir être considérée comme légale, la communication d'informations doit être suffisamment étayée par des informations fiables. Elle doit également être formulée avec précaution. Par exemple, aucune image sans nuance ne peut être donnée des renseignements sous-jacents, ou un élément particulier ne peut être présenté comme une 'vision de ' ou une 'impression de'. En ce sens, les informations fournies doivent également être 'justes' en offrant une image objective de la façon dont le service de renseignement perçoit la menace et le rôle de la personne concernée, sans être 'manipulatrices' […]* ».[127] Le Comité estimait que la note répondait au principe de précaution précité et que la VSSE avait, dans sa communication, suffisamment expliqué au gouvernement les

[127] COMITÉ PERMANENT R, Enquête de contrôle sur la manière dont les services de renseignement belges communiquent avec un employeur, privé ou public, sur un collaborateur, 2020.

raisons pour lesquelles les liens de la commissaire du gouvernement avec les Frères musulmans étaient susceptibles de représenter une menace.

Bien qu'une note écrite ait été préparée, il a été décidé, dans les jours qui suivent, de ne pas envoyer cette note directement. À la VSSE, l'on avait conscience que la note était politiquement sensible, incomplète, et qu'il fallait éviter une fuite. Il a été décidé d'informer oralement le ministre de la Justice, mais l'entretien n'a pas eu lieu. L'article 19 L.R&S ne stipule pas de quelle manière les renseignements doivent être communiqués par la VSSE. Par le passé, le Comité était d'avis que la communication devait se faire par écrit, et ce pour des raisons de sécurité juridique (excepté en cas d'extrême urgence), et ce afin d'éviter des discussions par la suite et permettre un contrôle parlementaire (voire juridique). La Secrétaire d'État compétente n'a pas été informée directement, la VSSE ayant supposé que le Premier ministre ou le Vice-Premier ministre s'en chargerait.

I.11.2.3. Aucune autre constatation d'enquête ?

La VSSE était consciente – entre autres après la séance plénière de début juin 2021 au Parlement – de la sensibilité politique de la question de la nomination. Cela étant, il a été décidé d'attendre la confirmation des éléments repris dans la note avant d'envoyer celle-ci. La note a finalement été retenue plus d'un mois, la VSSE ne souhaitant pas être instrumentalisée. Il apparait néanmoins qu'aucune modification n'ait été apportée à la note qui a finalement été envoyée en juillet au Premier ministre, aux Vice-Premiers ministres et à la ministre de l'Intérieur. En d'autres termes, il n'y a pas eu d'autre constatation d'enquête.

Sur la base des éléments de l'enquête, le Comité permanent R n'a pas pu se prononcer sur un lien de causalité entre la note et la démission de la commissaire de gouvernement Ihsane Haouach.

I.11.2.4. La fuite d'une note classifiée

La note sur Ihsane Haouach a été classifiée 'Confidentiel Loi 11.12.1998'. Elle a néanmoins été publiée *in extenso* dans la presse à peine un jour après sa transmission au Premier ministre, aux Vice-Premiers ministres et à la ministre de l'Intérieur. Dès lors que la remise d'un document classifié à un tiers constitue une infraction pénale, la VSSE a, à juste titre selon le Comité, porté plainte contre X auprès du procureur du Roi de Bruxelles.

Le Comité permanent R a rappelé qu'il appartient aux officiers de sécurité des différents cabinets ministériels de veiller à l'utilisation adéquate de documents classifiés. Les destinataires des notes classifiées doivent également être extrêmement prudents avec ces informations. Ils doivent tout d'abord être conscients que la remise à un tiers non habilité est un fait punissable sur le plan pénal. Pareille action peut également être dommageable pour les personnes faisant l'objet de la note.

Enfin, cela préjudicie également aux services de renseignement et porte atteinte à la confiance que leur accordent les citoyens.

I.11.2.5. Une 'entrave' ?

Dans la note destinée au ministre de la Justice, il était proposé d'organiser également un 'briefing de sensibilisation' pour Ihsane Haouach. La finalité sous-jacente était double. Il n'était pas exclu que l'intéressée elle-même n'était pas (pleinement) consciente d'entretenir des liens étroits avec les Frères musulmans, une sensibilisation était par conséquent nécessaire/utile. Si toutefois elle en était consciente, l'objectif de ce genre de briefing pouvait être de créer un effet perturbateur (ici en l'occurrence 'dissuasif'). La VSSE affirmait à ce propos qu'elle entendait à l'avenir adopter une approche disruptive, et ce, en élaborant des procédures et des accords de coopération. La question qui se posait était de savoir si l'initiative d'entrave doit/peut émaner d'un service de renseignement et de sécurité. Cette question, comme le respect de la note de service 'entrave' (il n'y a finalement pas eu d'entrave) n'a pas fait l'objet d'enquête.

I.11.2.6. La nécessité d'un screening pour les fonctions revêtant un caractère public ?

La VSSE a-t-elle ou devait-elle prendre l'initiative (spontanée) d'informer le gouvernement lorsqu'elle a pris acte de la nomination de Ihsane Haouach comme commissaire du gouvernement ? Ceci s'applique-t-il tout autant pour d'autres fonctions revêtant un caractère public ? [128] Tout un chacun peut-il faire l'objet d'une vérification ou un extrait du casier judiciaire suffit-il (anciennement le certificat de bonne vie et mœurs) ? La VSSE ne procède pas systématiquement à une vérification lors de chaque nomination d'un commissaire du gouvernement ou de toute autre fonction publique. Il est vrai que dans le cadre des enquêtes effectuées par le service, une personne assumant une fonction publique apparaît de temps à autre. Il convient alors de s'interroger sur l'opportunité de rédiger une note concernant cette personne. La VSSE n'est pas demandeuse d'émettre systématiquement un avis dans ce contexte. Il s'agit d'une décision qui, le cas échéant, doit être prise au niveau politique.[129]

---

[128] Voir en ce sens les problèmes relatifs à la désignation/démission de Salah ECHALLOUI à la Grande Mosquée de Bruxelles et au sein de l'Exécutif des musulmans (avis négatif de la VSSE).

[129] *Cf.* Note classifiée 'CONFIDENTIEL Loi 11.12.1998' de la VSSE du 25 août 2021 adressée au président du Comité permanent R.

Il convient de toujours garder à l'esprit le risque d'instrumentalisation quand il est question d'un sujet politiquement sensible. La structure des notes doit être adaptée à cet effet (ce travail était en cours) : les analystes doivent notamment expliciter la finalité d'une note, les hiatus, les éléments à préciser, ainsi que les personnes à qui la note doit être transmise.

I.12. UNE ATTENTION RENOUVELÉE POUR FRÈRES MUSULMANS

Le 19 juillet 2021, la Commission de suivi a demandé au Comité permanent R de réaliser une enquête de contrôle visant à déterminer, d'une part, si la confrérie des Frères musulmans faisait l'objet d'un suivi par la VSSE et le SGRS, et d'autre part, si elle était constitutive, selon ceux-ci, d'une menace en Belgique.[130] Cette enquête s'inscrivait dans le prolongement de l'enquête de contrôle réalisée sur la manière dont la VSSE a assuré le suivi de la commissaire de gouvernement de l'époque, Ihsane Haouach.[131]

I.12.1. LES FRÈRES MUSULMANS : CONTEXTUALISATION

I.12.1.1. Genèse et internationalisation du mouvement

La confrérie des Frères musulmans (en abrégé 'les Frères musulmans') trouve son origine en Egypte où elle fût fondée, en 1928, par Hassan Al-Banna. L'organisation poursuit à sa genèse deux objectifs : libérer l'Egypte de la domination britannique et réinstaurer les valeurs de l'Islam au sein de la société égyptienne. Elle est interdite en Egypte en 1948 après une série d'affrontements entre une fraction du mouvement et le pouvoir en place.

Très rapidement après sa fondation, le mouvement s'internationalise. Il se développe notamment en Europe suite à l'exil de plusieurs de ses leaders politiques.

---

130 Deux enquêtes de contrôle ayant trait à cette problématique avaient déjà été réalisées par le Comité permanent R. En 2001, le Comité a mené une enquête de contrôle visant à examiner la manière dont les services de renseignement recueillaient et analysaient des informations relatives au terrorisme et à l'islamisme radical, et la manière dont ils informaient les autorités civiles et judiciaires de ce phénomène. Cette enquête s'était notamment intéressée à la présence des Frères musulmans en Belgique, et au suivi qui en était fait par la VSSE. (COMITÉ PERMANENT R, *Rapport d'activités 2001*, 82-131). En 2007, le Comité a mené une enquête de suivi visant à déterminer si les recommandations formulées dans le cadre du suivi de l'islamisme radical par les services de renseignement avaient été suivies (COMITÉ PERMANENT R, *Rapport d'activités 2007*, 7-29).

131 Voir 'I.11 Le suivi d'un commissaire du gouvernement par la VSSE'.

Les Frères musulmans sont présents à partir des années 1960 en Belgique, où ils se sont progressivement investis dans des activités sociales, religieuses et de jeunesse.

I.12.1.2. Quelle ampleur du phénomène en Belgique ?

Pour pouvoir déterminer l'ampleur d'un phénomène, il faut d'abord pouvoir le définir. Le Comité a pu constater qu'il n'existait pas de définition précise et communément acceptée par les services de renseignement belges et les partenaires de la chaine pénale au sens large des « Frères musulmans ». Il s'agit d'une entité aux contours flous, disposant d'antennes jouissant d'une autonomie importante dans de nombreux pays et prenant la forme de différentes organisations opérant de manière discrète voire secrète dans divers pans de la société, et avec des objectifs à long terme incompatibles avec l'ordre démocratique. La difficulté à circonscrire cette mouvance rend son étude, et en particulier l'analyse de sa présence et de son pouvoir d'influence en Belgique, complexe. Il est également extrêmement difficile de déterminer l'appartenance d'une personne à ce groupement, puisque ce dernier ne dispose pas en tant que tel de structures précises ni ne distribue de carte de membre.[132]

La VSSE a néanmoins procédé à une estimation de la présence du mouvement en Belgique indiquant que « *les 'Frères musulmans internationaux' sont représentés par une organisation, la Ligue des Musulmans de Belgique (LMB), qui compterait seulement une cinquantaine de membres et une centaine de partisans ou sympathisants. Notre pays abrite également le siège de Council of European Muslims (CEM ; l'ancien FIOE [Federation of Islamic Organizations in Europe]), une organisation faîtière européenne qui défend les intérêts des Frères musulmans auprès des institutions européennes* ».[133]

Sur la base de ces chiffres, le ministre de la Justice a qualifié la présence du mouvement en Belgique comme « relativement modeste ».[134] Néanmoins, le ministre et la VSSE précisaient que les Frères musulmans paraissent être 'plus influents et plus importants que ce à quoi l'on pourrait s'attendre au vu de leur nombre limité de membres' en raison de leur activisme social et politique intense, leur approche et le profil de leurs membres.[135]

---

132 Le Comité avait déjà pu relever cette difficulté dans son rapport d'activités 2001 (COMITÉ PERMANENT R, *Rapport d'activités 2001*, 103).

133 VSSE, *Rapport annuel 2020*, 13.

134 Réponse du Vice-Premier ministre et ministre de la Justice et de la Mer du Nord datée du 10 mai 2021 à la question écrite n° 7 – 1140 du sénateur Tom ONGENA du 5 mars 2021.

135 *Ibid.* ; VSSE, *Rapport annuel 2020*, 13.

I.12.1.3. Une mouvance considérée comme une menace à l'étranger ?

Le positionnement des États à l'égard du mouvement varie fortement. Dans certains pays, des partis politiques se réclamant de la mouvance frériste sont au gouvernement ou dans l'opposition parlementaire (p. ex. en Turquie, au Maroc, en Algérie et en Lybie). Dans d'autres pays, ladite mouvance est criminalisée.[136] Par l'adoption de sa nouvelle loi antiterroriste le 8 juillet 2021, l'Autriche est le premier pays européen à interdire les Frères musulmans au titre d'organisation liée à la « criminalité à motivation religieuse ». Sans être criminalisé, le mouvement a également retenu récemment l'attention de nos pays voisins.[137]

I.12.2. CONSTATATIONS DE L'ENQUÊTE

I.12.2.1. La mouvance fait-elle l'objet d'un suivi par les services de renseignement ?

L'enquête a révélé que les deux services de renseignement opéraient un suivi des Frères musulmans selon des angles et avec des moyens humains et techniques très différents.

---

136 En Egypte, en Russie, en Arabie Saoudite, aux Emirats Arabes unis et au Bahreïn, elle est considérée officiellement comme une organisation terroriste.

137 Aux Pays-Bas, à l'initiative du Parlement, une enquête a ainsi été réalisée en 2019-2020 sur l'influence qu'exercent certains pays étrangers dans le sillage des Frères musulmans notamment pour infléchir leur démocratie (*Tweede Kamer der Staten-generaal, (On)zichtbare invloed, verslag parlementaire ondervragingscommissie naar ongewenste beïnvloeding uit onvrije landen, Den Haag, 25 juin 2020, consultable en ligne :* https://www.tweedekamer.nl/kamerstukken/detail?id=2020Z12034&did=2020D25817).
Les résultats de cette étude confirment l'exercice − sous diverses formes − d'une influence par plusieurs mouvances, dont celle des Frères musulmans. Il est renvoyé également à une étude réalisée par le service de renseignement néerlandais Algemene Inlichtingen- en Veiligheidsdiensten (AIVD) sur les Frères musulmans en 2011 concluant que les Frères musulmans ne représentaient pas de menace directe pour l'ordre démocratique ou la sécurité nationale mais que leurs activités pouvaient représenter à long terme un risque dès lors que les Frères musulmans sont anti-démocrates et opposés au processus d'intégration. En France, la présence des Frères musulmans et la menace qu'ils représentent ont également été étudiées dans le cadre d'une commission d'enquête du Sénat français lancée en novembre 2019 (*Rapport n° 595 (2019-2020), 7 juillet 2020, n° 595, consultable en ligne :* https://www.senat.fr/rap/r19-595-1/r19-595-1_mono.html#toc62). Dans ce rapport, on lit que le mouvement frériste compte en France environ 50 000 personnes. En Allemagne, les réponses du Gouvernement fédéral à plusieurs questions parlementaires nous apprennent que les organisations entretenant un lien avec les Frères musulmans sont observées par le service de sécurité nationale, le *Bundesambt für Verfassungsschutz* (BfV) et par tous les bureaux des Länder (*Ländesamts für Verfassungsschutz*). Une augmentation du nombre de membres et sympathisants à la confrérie des Frères musulmans dans le pays a été observée, passant de 1040 en 2018 à 1350 en 2019 (*Bundesam für Verfassungsschutz, Verfassungsschutzbericht 2019,* www.verfassungsschutz.de/SharedDocs/publikationen/DE/2020/verfassungsschutzbericht-2019.pdf?_blob=publicationFile&v=10, 180-181).

La VSSE réalise un suivi prioritaire de la mouvance dans le cadre de ses compétences pour le suivi de la menace extrémiste (art. 7, 1° & art.8, 1°, c L.R&S) et conformément aux objectifs stratégiques 2021-2024 fixés pour le service[138] et aux accords conclus entre la VSSE et le SGRS.[139] La VSSE collecte de l'information sur les Frères musulmans, les organisations et les personnes y liées, notamment par la mise en œuvre de méthodes de renseignements ordinaires (notamment des sources humaines) mais aussi des méthodes de renseignement particulières. Elle en extrait des renseignements qu'elle diffuse aux autorités et partenaires à titre d'information et de sensibilisation. Elle suit de près la problématique et a réorienté des capacités pour l'exercice de cette mission.[140]

Le SGRS étudie uniquement la mouvance dans le cadre de l'influence que celle-ci pourrait exercer au sein de la Défense conformément à ses compétences (art.11 L.R&S) et aux plans stratégiques. Il procède à une veille active en réceptionnant les informations produites par des tiers, mais il ne collecte pas proactivement des informations sur la mouvance dans sa globalité. Au terme de l'enquête, il est difficile de se prononcer sur la qualité de la position d'information du SGRS. Il est évident que les moyens déployés pour la collecte et l'analyse sont moins importants que ceux de la VSSE dès lors que – à la différence de la VSSE qui réalise un suivi du phénomène dans sa globalité – le SGRS étudie la mouvance fériste uniquement dans le cadre de l'influence que celle-ci pourrait exercer au sein de la Défense. Néanmoins, le Comité a relevé une inadéquation entre le niveau de priorité accordé au suivi du phénomène par le SGRS et les moyens déployés par le SGRS pour la collecte et l'analyse des données. Enfin, le Comité a constaté, sur la base des informations qu'il a réceptionnées, que le SGRS n'a pas pris l'initiative de diffuser des renseignements relatifs aux Frères musulmans aux autorités ou partenaires au cours des trois dernières années.

I.12.2.2. La mouvance est-elle identifiée comme une menace pour la Belgique ?

La VSSE et la SGRS présentent des conclusions similaires. Aucune menace immédiate n'a été détectée contre une institution spécifique directement liée à la mouvance des Frères musulmans. Néanmoins, la VSSE qualifie les Frères

138 Il y est indiqué que la lutte contre le terrorisme demeure une priorité mais que la VSSE ambitionne également de porter davantage d'attention à d'autres dossiers et qu'elle en tiendra compte dans la répartition du personnel et des ressources.

139 De ces accords, il découle que pour les domaines du terrorisme, du radicalisme et de l'extrémisme, la VSSE dispose en Belgique d'une compétence générale, et le SGRS d'une compétence réduite aux aspects d'extrémisme et de terrorisme qui concernent des intérêts militaires ou qui concernent des militaires belges.

140 Le dossier fût réinvesti peu avant 2020 après que des capacités engagées jusque-là sur des dossiers de 'terrorisme et extrémisme' furent libérées.

musulmans comme un mouvement extrémiste[141] représentant une menace haute et prioritaire en ce sens qu'ils peuvent conduire à des comportements antidémocratiques, à la polarisation ou à la violation des droits fondamentaux. La VSSE précise « *Les Frères musulmans respectent les règles démocratiques et la loi, et poursuivent à court terme des objectifs supposés légitimes. Or le discours, les convictions et la vision adoptés en interne à plus long terme sont contraires au bon fonctionnement de l'ordre constitutionnel et de la démocratie* ».[142] Elle ajoute que « *Le prosélytisme ('dawa') représente le moyen le plus approprié pour y parvenir, par le biais, entres autres, de la prédication et de l'enseignement (religieux). Dans ce contexte, les Frères musulmans se considèrent comme une avant-garde élitaire appelée à rassembler et diriger différentes communautés musulmanes. Ils visent à occuper des positions sociales influentes afin de pouvoir changer la société occidentale 'de l'intérieur' et tentent également d'influencer la politique gouvernementale par différents moyens* ».[143]

Le SGRS considère que « *les Frères musulmans promeuvent par certains aspects une vision extrémiste de la religion* » et qu'ils « *représentent un danger en ce qu'ils militent activement, et souvent de façon non transparente, en faveur d'une vision identitaire de l'Islam et renforcent ainsi les clivages au sein de la société et des institutions* ». Le SGRS précise également qu'il est particulièrement attentif au risque d'entrisme des Frères musulmans au sein de la Défense. Au terme de l'enquête, le Comité ignorait cependant si le risque d'entrisme est jugé élevé par le SGRS.

I.12.2.3. Collaboration entre partenaires

I.12.2.3.1. Collaboration entre services de renseignement

L'enquête a révélé que les deux services de renseignement belges échangent avec les services de renseignement étrangers sur le phénomène de manière bilatérale et multilatérale.

Au niveau national, le Comité a pu constater que la collaboration se faisait essentiellement dans un sens, à savoir le partage d'informations de la VSSE vers le SGRS.

---

141 L'extrémisme vise « *les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux fondements de l'État de droit en ce compris le processus de radicalisation* » (art.8, 1°, c L.R&S).

142 VSSE, *Rapport annuel 2020*, p.13.

143 *Ibid.*, p.12.

I.12.2.3.2. Collaboration avec l'OCAM

Au regard de la qualification et du niveau de la menace attribués par les services de renseignement au mouvement, le Comité s'est par ailleurs intéressé – sans entrer dans les détails – à la question de savoir si l'OCAM étudiait également celui-ci.[144] Questionné à ce sujet, l'OCAM a répondu n'avoir jamais rédigé de note ou d'étude sur les Frères musulmans. L'OCAM n'identifiait par ailleurs pas de menace directe de cette mouvance pour la Belgique, et n'évoquait ni une menace à court ou moyen terme ni ne confirmait le caractère élevé de la menace contrairement à l'analyse des deux services de renseignement.

Interpellé par l'absence de vision conjointe entre, d'une part, la VSSE et le SGRS, et d'autre part, l'OCAM quant à la menace que représentent les Frères musulmans, le Comité a conclu qu'une concertation entre ces services s'avérait nécessaire. Il s'étonnait d'ailleurs qu'elle n'avait pas encore eu lieu étant donné la priorité accordée à ce dossier par la VSSE et par le SGRS.

I.12.2.4. Quelles stratégies poursuivent les services de renseignement pour endiguer la menace identifiée?

Afin de contrer la stratégie des Frères musulmans et éviter que la mouvance puisse s'installer dans une position de médiateur entre les communautés musulmanes et les autorités, la VSSE estime qu'il est capital d'investir dans la sensibilisation des autorités et administrations. Les initiatives prises et celles à venir témoignent de cette stratégie poursuivie par la Sûreté de l'État. Le service a diffusé deux notes dans un but d'information et de sensibilisation, l'une aux services de renseignement et aux services partenaires de la chaine pénale associés, et l'autre aux ministres compétents, et prévoyait d'en diffuser d'autres destinées, cette fois, à un public plus large.

Le SGRS indique que la sensibilisation des acteurs institutionnels aux tentatives d'influence par les Frères musulmans en dehors de la Belgique fait partie des objectifs des briefings donnés à ces acteurs institutionnels sur la menace terroriste et le risque lié aux mouvements radicaux religieux. Le Comité ne dispose pas d'informations supplémentaires lui permettant de se prononcer sur la quantité ou la qualité de ces briefings de sensibilisation.

À la clôture de l'enquête, le Comité a conclu qu'une concertation entre les services de renseignement et ses partenaires (l'OCAM, la Police fédérale, etc.) sur le phénomène constituait une étape cruciale pour la réussite et le renforcement de la stratégie de sensibilisation poursuivie. La sensibilisation des autorités politiques

144 L'OCAM est en effet compétent pour l'évaluation de la menace en matière d'extrémisme lorsque cette menace est susceptible de porter atteinte à la sûreté intérieure et extérieure de l'État, aux intérêts belges et à la sécurité des ressortissants belges à l'étranger ou à tout autre intérêt fondamental du pays (art.3 L.OCAM).

et des administrations sera d'autant plus efficace si elle est portée par l'ensemble de ces services qui se sont préalablement accordés sur une définition commune du phénomène et sur la menace qu'il représente pour la Belgique.

I.13. LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION DANS LE PROCESSUS DE RENSEIGNEMENT AU SEIN DE LA DIRECTION CYBER DU SGRS ET AU SEIN DE LA VSSE

I.13.1. LE CORE BUSINESS D'UN SERVICE DE RENSEIGNEMENT

Les technologies de l'information et de la communication (TIC ou ICT en anglais) jouent un rôle de plus en plus important dans les processus de renseignement, aussi bien dans la collecte et l'analyse des informations (par exemple, les écoutes (SIGINT) ou encore les prises d'images (GEOINT)) que dans la diffusion des renseignements. L'augmentation constante des flux de données nécessite des systèmes adéquats, prêts à absorber ces flux et permettant une analyse correcte, rapide et efficace. L'environnement informatique doit donc être un outil stable et orienté vers l'avenir, et ce afin de soutenir les différents acteurs intervenant dans le cycle du renseignement. Cet environnement, aussi bien matériel ('*hardware*') que logiciel ('*software*') doit se conformer aux standards en la matière, aux bonnes pratiques IT, tout en tenant compte des nouvelles et futures évolutions technologiques[145], telles que le '*big data*'.[146]

Dans des enquêtes antérieures, le Comité permanent R avait constaté que les services de renseignement étaient confrontés à des défis majeurs dans ce domaine. Surtout pour le SGRS, il est déjà apparu par le passé que l'ICT était un point d'attention. Le Comité avait relevé que les activités de renseignement n'étaient

[145] Les organes de contrôle ont aussi un rôle important à jouer à cet égard. Voir à ce propos : K. VIETH et T. WETZLING, *Data-driven Intelligence Oversight. Recommendations for a System Update*, Stiftung NeueVerantwortung, novembre 2019, 63 p.

[146] La notion de '*big data*' fait référence à la science qui consiste à collecter et analyser de grands volumes de données dans le but de découvrir certains '*patterns*' intéressants sur la base d'une classification ('*clustering*') et d'analyses statistiques permettant ainsi de fournir une aide à la décision. Ces données sont généralement caractérisées par une variété, une vélocité et un volume importants.

pas (ou plus) suffisamment soutenues par l'ICT et que les conditions d'une bonne gestion de l'information n'étaient pas (ou plus) complètement remplies.[147] [148]

Par conséquent, le Comité permanent R a initié, en mai 2019, une 'enquête de contrôle sur les moyens informatiques utilisés par les services de renseignement belges pour la collecte, le traitement, l'analyse et la communication de l'information dans le cadre du cycle du renseignement'. L'enquête se concentrait sur les moyens informatiques spécifiquement utilisés en soutien au cycle du renseignement. Il s'agit des systèmes qui sont utilisés, par exemple, pour la collecte d'informations, ou encore des outils d'analyse et bases de données spécifiques. Le Comité permanent R ne s'est pas penché sur les outils bureautiques génériques utilisés par les services (par ex. Windows, Word, Excel, etc.), dans la mesure où ils ne sont pas spécifiques aux services de renseignement. Le Comité n'a pas non plus examiné en détail le matériel informatique ('*hardware*') à la disposition des services, à moins qu'il ne soit spécifique au service de renseignement concerné.

Le premier volet de l'enquête portait sur le SGRS, et ce en raison de l'impact de la restructuration de ce service sur les outils ICT et les méthodes de travail. L'enquête ayant été finalisée en mai 2020, les résultats ont été présentés dans le rapport d'activités de l'année 2020.[149]

Les deuxième et troisième volets concernaient la direction Cyber du SGRS et la VSSE. Les résultats de ces deux volets sont discutés dans le présent chapitre.

Les questions d'enquête principales, soumises à la VSSE et à la direction cyber du SGRS, étaient les suivantes :

- Quelles sont les technologies et quels sont les outils utilisés par le service/la direction pour soutenir les activités de renseignement?
- Dans quelle mesure les instruments sont-ils développés en interne ou fournis par des partenaires externes ?
- Les 'bonnes pratiques' usuelles (ci-après 'ITIL')[150] sont-elles appliquées correctement? (plus précisément: '*change management*', '*inventory management*', '*business continuity*', '*incident management*', '*problem management*', etc.) ?

147 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 7-14 ('II.1. Un audit au sein du service de renseignement militaire') ; *Rapport d'activités 2018*, 2-18 ('I.1. Le fonctionnement de la Direction Counterintelligence (CI) du SGRS').

148 Le rapport de la Commission d'enquête parlementaire en réponse aux attentats de Zaventem et Maelbeek recommandait également de renforcer la gestion de l'information des services de renseignement, plus particulièrement pour garder la surinformation ('infobesitas') sous contrôle. Voir 'Commission d'enquête sur les attentats terroristes du 22 mars 2016. *Doc. parl.* Chambre, 2016-2017, n° 54-1752/008, 15 juin 2017, p. 53 et 180 et suiv.

149 COMITÉ PERMANENT R, *Rapport d'activités 2020*, (I.6 « Les technologies de l'information et de la communication dans le processus de renseignement au SGRS »), 33 et suiv.

150 ITIL est l'acronyme de '*Information Technology Infrastructure Library*', qui se traduit par 'Bibliothèque pour l'infrastructure des technologies de l'information'. Il s'agit des bonnes pratiques pour la gestion des services IT les plus utilisés au monde (source: www.heflo.com/fr/blog/technologie/definition-itil).

- Existe-t-il une politique de *'business continuity plan*' (BCP) ainsi que des procédures *'disaster recovery plan*' (DRP) prévoyant les backups et sont-elles actualisées ?[151]
- Les outils sont-ils tous inscrits dans un registre des traitements de données à caractère personnel disponible pour le Comité permanent R comme prévu par la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ?

L'enquête visait à identifier les risques[152] auxquels sont confrontés les deux services de renseignement et, par le biais de recommandations, à maitriser ces risques. À partir du modèle dit 'CIA'[153], trois types de risques ont été investigués :
- *Confidendiality* : le risque de prise de connaissance de données, classifiées ou non ;
- *Integrity :* le risque de modification non autorisée de données, classifiées ou non ;
- *Availability* : le risque que les données ne soient pas disponibles, ce qui empêcherait de mener à bien les missions du service.

I.13.2. L'ENVIRONNEMENT ET L'ORGANISATION ICT DE LA DIRECTION CYBER DU SGRS

I.13.2.1. Contexte

I.13.2.1.1. Équipe et personnel

L'informatique à la direction Cyber du SGRS est gérée par une équipe dédiée à cette fin, étant donné qu'il s'agit du *core business* de cette direction.

Fin mars 2021, les effectifs ICT cyber étaient insuffisants : il y avait 80 % d'effectifs ICT engagés par rapport aux postes prévus. Le turnover du personnel,

---

151 Il existe de bonnes pratiques généralement acceptées sur la manière la plus optimale d'effectuer des sauvegardes et sur les procédures à appliquer en cas de désastre. La gestion des backups s'inscrit, tout comme les procédures DRP (*'disaster recovery plan*'), dans un *'business continuity plan*' (BCP) global.

152 Un 'risque' a été défini comme étant l'éventualité de l'existence d'une défaillance ou d'une menace plus ou moins prévisible pouvant influencer la réalisation des objectifs d'une organisation ou l'accomplissement efficiente de ceux-ci, associé à la probabilité que survienne un événement nuisible suite à cette défaillance.

153 L'utilisation du modèle dit 'CIA' est préconisée comme base d'analyse de risques selon les normes internationales ISO 270 relatives à la sécurité de l'information.

non négligeable, est principalement dû aux changements de personnel du cadre E-Gov[154], mais aussi à des départs de civils.[155]

La 'capacité serveurs' (ou ressources physiques) était suffisante au moment de l'enquête mais ne répondait pas aux ambitions à long terme du service. Des acquisitions étaient prévues, mais dépendaient des attributions budgétaires et, de ce fait, des priorités imposées au service.

Concernant le recours à la sous-traitance et aux marchés publics, la division Cyber dispose de personnel soit militaire, soit civil engagé via Selor ou mis à disposition via des contrats E-Gov Select. Étant donné que la grande majorité des logiciels provient du monde open-source, il n'y a pas de recours systématique à de la sous-traitance ou à des marchés publics d'achat de logiciels. Les développements se font, quant à eux, en interne.

I.13.2.1.2. Serveurs et réseaux

L'accès aux salles serveurs s'effectue via un mécanisme sécurisé. Des backups sont effectués régulièrement.

Une base de données de gestion de configuration (CMDB)[156] existe et est mise à jour manuellement. Il serait préférable que cette CMDB soit mise à jour automatiquement afin d'être certain de l'exactitude des données, mais également afin de détecter des anomalies.

Le monitoring est effectué par différents logiciels. Cependant, la multiplication de ces logiciels pourrait avoir un effet négatif sur la réactivité par rapport à une alerte. Il serait dès lors intéressant de se concentrer sur un logiciel central.

I.13.2.1.3. Logiciels impliqués dans la mission de renseignement

En ce qui concerne les principaux systèmes logiciels impliqués dans le cycle du renseignement, le Comité a pu constater que la division Cyber a construit toute son infrastructure en s'appuyant sur un plan stratégique à long terme et sur des domaines d'activités précis. De plus, aussi bien pour le côté matériel que logiciel, elle s'efforce de suivre les bonnes pratiques 'ITIL'.

---

154 E-gov est actif dans le recrutement et la sélection d'informaticiens spécialisés pour des services publics et institutions.

155 Le personnel de Cyber est composé de militaires, de fonctionnaires sous statut Camu et d'externes engagés via E-Gov Select.

156 Il s'agit d'une base de données – appelée Component Management DataBase (CMDB) – reprenant tous les composants ICT aussi bien les réseaux (switchs, routeurs, etc.) que les systèmes (serveurs, pc, etc.) et logiciels. Lorsque l'infrastructure informatique devient plus complexe, il est important d'exploiter une base de données de ce type car elle permet d'assurer un suivi de l'information au sein de l'environnement informatique.

Le nombre d'applications métier utilisées par la direction Cyber est conséquent et englobe tout le spectre de ses missions. Le Comité permanent R a choisi d'examiner un ensemble représentatif de ces applications.[157]

Les constats principaux sont les suivants :

- Il existe peu d'outils de type *big data* et *datamining* étant donné que les missions de Cyber (recherche et analyse de menaces, sensibilisation, protection des réseaux, etc.) ne le nécessitent pas. Cependant, certains outils disposent de mécanismes internes pouvant s'y apparenter.
- Le registre des traitements tel qu'exigé par la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel était en cours de construction pour les applications gérées par la direction Cyber.[158] Celui-ci n'était pas entièrement opérationnel, mais les adaptations à effectuer étaient mineures.
- Le Comité a pu constater que le réseau Cyber est stable et rapide. Un monitoring du réseau ainsi que de l'infrastructure en général est en place et permet de détecter les pannes.
- Les backups sont effectués régulièrement. Un processus DRP existe pour les applications principales. Celui-ci devrait être complété et mis à jour au fur et à mesure des changements effectués sur l'infrastructure.

I.13.2.1.4. Test de vulnérabilité et sécurité

Le Comité a pu constater qu'aussi bien pour les outils développés en interne que ceux acquis, une attention particulière est donnée aux aspects de sécurité et de test des applications. Celles-ci sont soumises à une série de tests automatiques et manuels, en utilisant à cet effet des produits reconnus sur le marché pour leur efficacité.

La sécurité a également été prise en compte lors de l'implémentation physique de l'infrastructure.

Enfin, les analyses d'éléments potentiellement nuisibles (tels qu'un *possible malware*) sont réalisées dans des environnements sécurisés.

I.13.2.2. Évaluation des risques

Différents points d'attention ont été énumérés pour chaque section de l'organisation ICT de la Direction Cyber du SGRS. Au cours de cette enquête, le Comité a mis

---

157 Les applications qui n'ont pas été choisies pour une démonstration sont soit similaires aux applications exposées, soit bien connues dans le monde IT. Une préférence a également été donnée aux applications développées en interne ou aux équipements nécessitant la création de scripts spécifiques par le personnel de la division Cyber.

158 Ce registre doit permettre au Comité permanent R (en tant qu'autorité de protection des données) de connaître à tout moment les traitements sur données personnelles effectués ainsi que les types de données, les durées de rétention et les responsables du traitement.

en évidence certains risques, leur probabilité ainsi que les pistes d'atténuation ('*mitigation*') afin de réduire ces risques.[159] Parmi les risques les plus importants encourus par le service, le Comité a insisté sur les points suivants :
- Le manque de personnel et la rotation dans le personnel ;
- Le renforcement de l'infrastructure physique ;
- Les outils de monitoring du réseau ;
- Les collaborations avec les firmes externes.

I.13.3. L'ENVIRONNEMENT ET L'ORGANISATION ICT DE LA VSSE

I.13.3.1. Contexte

I.13.3.1.1. Équipe et personnel

L'informatique à la VSSE est gérée par une équipe réduite. Son rôle est central, car elle offre un appui aux différents services et bureaux qui récoltent, analysent et disséminent les informations et renseignements.

En date du 1er juin 2021, les effectifs ICT étaient insuffisants. Cela est d'autant plus vrai pour le nombre de développeurs qui est extrêmement faible.

Concernant le recours à la sous-traitance et aux marchés publics, la VSSE exige une habilitation de sécurité pour les soumissionnaires. Les développements software se font souvent par des externes via des marchés publics ou sont en réalité des acquisitions. Les développements commandés via marchés publics ne donnent cependant pas nécessairement satisfaction : retard sur les délais, spécifications et technologies changeantes, dépassement des budgets, etc.

I.13.3.1.2. Serveurs et réseaux

Les salles serveurs et les systèmes de backups correspondent à des standards de sécurité élevés, sont efficaces et ont été conçus suite à une analyse de risques spécifique renouvelée régulièrement.

Une base de données de gestion de configuration (CMDB) existe et est mise à jour manuellement. Il serait préférable que cette CMDB soit mise à jour automatiquement afin d'être certain de l'exactitude des données, mais également afin de détecter des anomalies.

La gestion des configurations ainsi que le monitoring sont réalisés par un outil commercial s'intégrant à l'ensemble de l'architecture et se font sur les points

[159] La confidentialité ne permet pas de détailler cette analyse de risques dans ce rapport d'activités public.

de contrôle les plus critiques (applications, matériel, réseau, ...). Cet outil est de qualité mais pourrait être plus performant en termes de détection de problèmes en agissant de manière proactive.

I.13.3.1.3. Logiciels impliqués dans la mission de renseignement

En ce qui concerne les principaux systèmes logiciels impliqués dans le cycle du renseignement, le Comité a pu constater que la VSSE utilise une seule base de données « métier ». D'autres bases de données peuvent exister en tant que composant d'applications mais ne sont que des bases de données techniques permettant le travail de ces applications. Cette base de données métier a été régulièrement améliorée et récemment migrée vers une technologie plus moderne.

Pour la modernisation de la base de données « métier » début 2020, l'option retenue est la consolidation et la réorganisation des bases de données (de type SQL) avec l'ajout d'index de recherches. Cette méthode peu onéreuse fournit des résultats satisfaisants pour les opérations les plus courantes.

Le projet Atlas, débuté en 2015 (dossier budgétaire) et 2017 (développement) avec comme livraison finale prévue fin 2021, opte pour une autre approche, celle de l'utilisation de nouveaux types de bases de données axées sur la présence ou non d'éléments (données, tags) permettant d'établir un score de pertinence de l'information.[160] Ce projet, réalisé en collaboration avec la firme Smals, correspond aussi aux prescrits de l'analyse *big data*. Tous les composants du projet n'étaient pas encore livrés ou mis en production au terme de l'enquête. Le Comité permanent R a pu assister à une démonstration des fonctionnalités stables déjà développées. Le but de ce projet est de centraliser toutes les données de la VSSE, qu'elles proviennent ou non de l'extérieur. Il a été rapporté au Comité des problèmes concernant la prise en compte de certains besoins des utilisateurs, ainsi que des soucis de planning.[161]

Quant au registre des traitements tel qu'exigé par la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, il était en cours d'élaboration pour les applications gérées par la VSSE. Le Comité a pu constater que celui-ci n'était pas entièrement opérationnel, mais les adaptations à effectuer étaient mineures.

Le Comité a noté que le réseau était stable et rapide. Un monitoring du réseau ainsi que de l'infrastructure en général est en place et permet de détecter les pannes.

---

160 Il s'agit de bases de données '*no-sql*' qui ont une structure beaucoup plus simple et permettent des recherches sur des contenus de fichiers ou de tags.

161 Il apparait que la communication entre l'équipe de projet et les utilisateurs clés relayant des besoins spécifiques (notamment ceux liés aux BIM) est sommaire. Le projet Atlas souffrait également de retards dans son ensemble ainsi que d'un dépassement de budget. Ces retards et dépassements ne sont pas imputables à la VSSE. La Smals a rencontré certaines difficultés lors de l'implémentation, ce qui a augmenté le temps de travail et, de ce fait, le budget nécessaire. Des choix de priorité d'implémentation ont donc dû être opérés.

Néanmoins, ce monitoring est axé sur la détection de problèmes effectifs et non sur des recherches proactives.

Les backups sont effectués quotidiennement dans le respect des règles en la matière. Un processus DRP existe pour les applications principales. Les autres applications étant des éléments de support et fonctionnant en *stand-alone* sur des postes fixes, celles-ci ne nécessitent que la documentation fournie par la firme. Le processus DRP s'inscrit bien dans le cadre d'un plan BCP plus global.

Enfin, le Comité s'est penché sur plusieurs logiciels existants ou en développement, dont le projet Tardis (également appelé Bavak), lancé fin 2016. Ce logiciel, à développer, devait permettre d'automatiser les actions en ligne sur les différents réseaux sociaux, d'extraire les informations (avec une traduction automatique de celles-ci), de les analyser et de les exporter dans un rapport. Au fil du temps, le projet s'est complexifié au vu de plusieurs fonctionnalités qui ont été ajoutées. Ce projet a finalement été abandonné début 2021 par la VSSE après avoir constaté qu'il ne répondait pas aux attentes. En effet, les comptes des réseaux sociaux sur lesquels le logiciel opérait étaient rapidement supprimés car la présence du logiciel était détectée.[162]

I.13.3.1.4. Test de vulnérabilité et sécurité

Le Comité a pu constater que des tests de sécurité sont effectués sur les programmes développés en interne. Les autres applications sont soit issues du monde *open source*, soit commerciales. Pour certaines d'entre elles, il existe une certification, tandis que pour d'autres, il n'y a pas de garantie qu'un test d'intrusion ait été effectué. Cependant, les mises à jour fréquentes sont fournies et appliquées par la VSSE.

La VSSE travaille notamment avec un réseau sécuriré non connecté à internet et soumis à une homolgation de l'ANS.

Par ailleurs, une journalisation des activités sur les applications est effectuée (logging et actions des utilisateurs), permettant de disposer d'une preuve des activités des utilisateurs.

I.13.3.2. Évaluation des risques

Une série de points d'attention ont été énumérés pour chaque section de l'organisation ICT de la VSSE. Au cours de cette enquête, le Comité a mis en évidence certains risques, leur probabilité ainsi que les pistes d'atténuation

[162] Voir à ce propos notamment la Question de S. THEMONT au ministre de l'Intérieur sur 'Le logiciel de détectage de menaces terroristes ou de radicalisation' (*Q.R.*, Chambre, 2020-2021, 3 mai 2021, n°50, p.306, Q. n°456) ; la Question de V. SCOURNEAU au ministre des Affaires étrangères et de la Défense sur 'OSINT.' (*Q.R.*, Chambre, 2019-2020, 5 août 2020, n°24, p.465, Q. n°407).

('*mitigation*') afin de réduire ces risques.[163] Parmi les risques les plus importants encourus par le service, le Comité a insisté sur les points suivants :
– Le manque de personnel, et de certains profils en particulier ;
– Les communications sécurisées ;
– Le projet Atlas au regard des problèmes rapportés au Comité concernant le manque de prise en compte de certains besoins des utilisateurs ainsi que des soucis de planning (*supra*).

I.14. ENQUÊTES DE CONTRÔLE POUR LESQUELLES DES DEVOIRS D'ENQUÊTE ONT ÉTÉ EFFECTUÉS EN 2021 ET ENQUÊTES QUI ONT DÉBUTÉ EN 2021

I.14.1. L'APPLICATION DE NOUVELLES MÉTHODES (PARTICULIÈRES) DE RENSEIGNEMENT

Le Comité s'est vu attribuer une série de possibilités de contrôle en ce qui concerne certaines méthodes 'ordinaires'. Il s'agit notamment du contrôle de l'identification de l'utilisateur de télécommunications (art. 16/2 L.R&S), de l'accès à des données des dossiers passagers (*Passenger Name Record*, art. 16/3 L.R&S), de l'accès aux images des caméras utilisées par les services de police (art. 16/4 L.R&S), ou encore du contrôle préalable aux interceptions, aux intrusions dans un système informatique et la prise d'images animées (art. 44/3 L.R&S).

Le Comité a décidé d'étudier cette matière dans une enquête intitulée : *'enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R'*.

En 2020, l'accent a été mis sur l'élaboration d'une méthodologie dans le cadre du contrôle de l'identification de l'utilisateur de télécommunications (art. 16/2 L.R&S), ainsi que l'accès aux données PNR (art. 16/3).

Début 2021, le volet méthodologique relatif au contrôle préalable aux interceptions, aux intrusions dans un système informatique et à la prise d'images animées (art. 44/3 L.R&S) a été finalisé.

En 2021, le Comité s'est en outre penché sur l'opérationnalisation de l'article 16/4, §2 L.R&S. Cet article régit l'extraction rétroactive des images des caméras de police par les services de renseignement. Cette disposition législative a une portée générale. Cela implique que les exigences procédurales qui y sont énoncées sont d'application pour l'extraction ciblée des images des caméras de police par un accès direct (en ligne) aux banques de données de la police concernées ainsi que pour

[163] La confidentialité ne permet pas de détailler cette analyse de risques dans ce rapport d'activités public.

l'extraction ciblée via une requête écrite adressée au service de police compétent (à savoir la Direction de l'information policière et des moyens ICT (DRI)). En raison d'une plainte DPA, l'enquête a été interrompue. La plainte a conduit à la rédaction d''Instructions de traitement du Comité permanent R (APD) concernant les extractions rétroactives par les services de renseignement des images de caméras de police sur la base de l'article 16/4, §2 L.R&S' (traduction libre).[164] Après réception et analyse des statistiques des deux services de renseignement quant à l'utilisation de cette méthode, le rapport d'enquête sera finalisé en 2022.

I.14.2 LE SUIVI PAR LA VSSE DES CONDAMNÉS POUR TERRORISME QUI ONT ÉTÉ LIBÉRÉS

En Belgique, près de 500 personnes ont été condamnées pour des faits de terrorisme entre 2015 et 2021.[165] Certains condamnés l'ont été par contumace et n'ont donc pas pu être placés en détention. Une série d'autres ont obtenu une permission de sortie de prison et ont entre-temps purgé leur peine en prison ou ont été libérés sous conditions (avant la fin de la peine) suite à une décision du tribunal d'application des peines.

Compte tenu de l'inquiétude des services de renseignement belges et européens quant à une potentielle récidive, le Comité a décidé, à la mi-2019, d'ouvrir une enquête de contrôle sur *'le suivi par les services de renseignement et de sécurité belges, d'une part des inculpés en Belgique pour infractions terroristes perpétrées en Belgique ou ailleurs et bénéficiant d'une modalité visée par la loi du 20 juillet 1990 et d'autre part, des condamnés en Belgique pour infractions terroristes qui sortent de prisons belges, soit dans le cadre d'une des modalités visées dans le cadre de la loi du 17 mai 2006, soit qui sont libérés définitivement (art. 71 de ladite loi)'*.

Le Comité a examiné la manière dont les deux services de renseignement (VSSE et SGRS) suivent cette thématique, quels moyens et quelles méthodes sont utilisés, la manière dont se déroule la coopération avec les partenaires (entre autres l'OCAM, la Direction générale des Établissements pénitentiaires, la Police fédérale et locale, etc.) et au sein de quelles structures (Local Task Forces, Groupe de travail Prisons, etc.). Enfin, les approches française et anglaise ont été étudiées à travers un benchmarking.

En 2021, face aux premiers résultats, le spectre de l'enquête a été élargi. En effet, pour comprendre l'organisation du suivi *après* la libération de ces détenus, il est apparu nécessaire de s'intéresser également au suivi par les services de renseignement et de sécurité *pendant* la détention. Il a aussi été tenu compte des évolutions législatives et des nouveaux cadres de coopération, par exemple la

164 '*Verwerkingsinstructie van het Vast Comité I (DPA) m.b.t. de door de inlichtingendiensten ingestelde retroactieve opvragingen van politionele camerabeelden gegrond op artikel 16/4, §2 W.I&V*'.

165 *Doc. parl.* Chambre 2021-22, CRIV55PLEN148, 25.

publication par l'OCAM de la Stratégie Extrémisme et Terrorisme (dite Stratégie TER) en septembre 2021. L'enquête sera finalisée au premier semestre 2022.

I.14.3. LE RISQUE D'INFILTRATION AU SEIN DES DEUX SERVICES DE RENSEIGNEMENT

Le monde du renseignement, au niveau international, a été secoué ces dernières années par une série de cas d'infiltration (et '*insider threat*'). Le Comité a pris l'initiative de lancer une enquête de contrôle sur la manière dont les deux services de renseignement gèrent le risque d'infiltration : quels risques ont été identifiés ? Quelles mesures ont été prises pour les maîtriser et pour réagir si ces risques venaient à se concrétiser ?

Plusieurs réunions de travail ont été organisées avec le SGRS et la VSSE sur la thématique 'cartographie et évaluation du risque d'infiltration au sein des services de renseignement'. À cet égard, le processus de gestion du risque, tel que repris dans la norme ISO 31000, constituait une base de départ.[166]

Prévu en 2021, le traitement des informations récoltées a pris du retard, principalement en raison de la crise sanitaire et de son impact sur les effectifs du Comité ainsi que de la prise en charge de dossiers urgents (l'affaire Conings, *supra*).

I.14.4. MENACES ÉVENTUELLES POUR LE POTENTIEL ÉCONOMIQUE ET SCIENTIFIQUE (PRISM/PES) : ENQUÊTE DE SUIVI

En 2016, une enquête de contrôle relative à la protection du potentiel économique et scientifique, dans la foulée desdites 'révélations de Snowden', a été finalisée.[167] Ces révélations ont notamment donné un aperçu de l'existence du programme PRISM, au travers duquel la National Security Agency (NSA) américaine récoltait des (méta)données de télécommunication. Elles ont également révélé les opérations de renseignement montées par les services américains, mais aussi britanniques, contre certaines institutions internationales et structures de coopération (ONU, UE et G20). Des pays dits 'amis' étaient eux aussi visés. L'enquête portait sur les implications éventuelles des programmes étrangers sur la protection du potentiel économique et scientifique du pays. Il s'agissait de vérifier si les services de renseignement belges étaient attentifs à ce phénomène ; s'ils avaient détecté une menace réelle ou éventuelle contre le potentiel économique et scientifique belge ; s'ils avaient informé les autorités compétentes et leur avaient suggéré des mesures

166 www.iso.org:fr/iso-31000-risk-management.html

167 COMITÉ PERMANENT R, *Rapport d'activités 2016*, 52 et suiv.

de protection et, enfin, s'ils disposaient de moyens suffisants et adéquats pour suivre cette problématique. Le Comité a par ailleurs examiné les conséquences du programme PRISM et/ou de systèmes analogues sur le potentiel économique et scientifique du pays.

Fin novembre 2019, la Commission parlementaire de suivi a demandé au Comité permanent R de reprendre l'enquête de contrôle et de l'actualiser. En 2020, après des premiers devoirs d'enquête, en particulier la collecte et l'analyse de sources ouvertes, il a été décidé de fusionner cette enquête avec l'enquête de contrôle sur l'opération Rubicon (Voir I.14.5). En 2021, le Comité a rencontré et interrogé les deux services de renseignement à ce sujet. Des questions ont également été posées au Centre pour la Cybersécurité Belgique (CCB). Après l'analyse de ces réponses, la rédaction du rapport a toutefois été interrompue par la prise en charge d'enquêtes de contrôle urgentes et prioritaires, en particulier sur l'affaire Conings (Voir I.9). Les résultats de l'enquête sont attendus pour début 2022.

I.14.5. ESPIONNAGE VIA DU MATÉRIEL DE CRYPTAGE : L'OPÉRATION RUBICON

Mi-février 2020, des révélations ont été faites sur l''Operation Rubicon'[168], c'est-à-dire l'opération de renseignement par laquelle les services de renseignement américains et allemands ont, des décennies durant, écouté des communications cryptées émanant d'autorités dans des dizaines de pays, en utilisant la société suisse Crypto AG comme couverture.[169] Les Pays-Bas, la France, la Suède et le Danemark (les 'pays Maximator'), entre autres, étaient '*cognescenti*', c'est-à-dire initiés aux détails cryptologiques de certains appareils. La Belgique, "*précieuse pour les éclaircissements que ses rapports apportaient sur les événements diplomatiques*" (traduction libre)[170] et surtout intéressante comme centre diplomatique de l'OTAN et de ce qui était à l'époque la Communauté économique européenne, aurait notamment été visée.

---

168 La revue *Intelligence and National Security* (Volume 35, August 2020, Issue 5) y a consacré un numéro thématique. Voir notamment : R. ALDRICH et al., 'Operation Rubicon: sixty years of German-American success in signals intelligence'; M.J. DOBSON, 'Operation Rubicon: Germany as an intelligence 'Great Power" et B. JACOBS, 'Maximator: Europan signals intelligence cooperation from a Dutch perspective'.

169 Les rapports d'évaluation des services de renseignement américains et allemands ont été publiés par la chaîne de télévision allemande ZDF et le Washington Post. La plateforme de recherche néerlandaise Argos a pu consulter les rapports, qui ont notamment été repris par De Tijd (L. BOVÉ, *De Tijd*, 13 février 2020, ('Geheime documenten onthullen spionage van België door CIA en Duitse BND')).

170 *«waardevol voor de verheldering die zijn rapporten bood over diplomatieke gebeurtenissen ».*

Le Comité a décidé d'ouvrir une enquête de contrôle, tentant d'apporter une réponse à des questions telles que[171] : dans quelle mesure les services de renseignement belges étaient-ils au courant (ou dans quelle mesure devaient-ils l'être) de ces opérations compte tenu de leurs missions légales ? Des renseignements ont-ils été recueillis à ce propos ou cela n'a-t-il pas été jugé souhaitable ? Mais plus important encore : les services offrent-ils actuellement une protection suffisante en la matière ? Des analyses de risques ont-elles été effectuées ? En cas d'utilisation avérée de matériel du cryptage, quelles mesures de précaution ont alors été prises ? Comment cette problématique de cryptage est-elle gérée aujourd'hui ? Fin septembre 2020, il a été décidé de fusionner cette enquête avec l'enquête de suivi PRISM/PES (Voir I.14.4).

I.14.6. CAPACITÉS DE RENSEIGNEMENT (SUPPLÉMENTAIRES) À L'ÉTRANGER POUR LES SERVICES DE RENSEIGNEMENT BELGE ?

Compte tenu de la mission de renseignement décrite par le législateur, les informations pertinentes pour les services de renseignement se trouvent à la fois en Belgique et à l'étranger. Par conséquent, une enquête de contrôle a été ouverte en 2020 sur 'les capacités de renseignement (supplémentaires) des services de renseignement belges à l'étranger'. Cette enquête poursuit divers objectifs :

- Vérifier si la VSSE et/ou le SGRS procèdent actuellement à un recueil opérationnel d'informations à l'étranger, et dans l'affirmative, sous quelle forme et par le biais de quelles activités de renseignement ;
- Examiner les activités menées à l'étranger sous l'angle du cadre réglementaire en vigueur ;
- Vérifier si les services ont besoin de moyens supplémentaires, parmi lesquels des moyens juridiques (en d'autres termes, des compétences d'enquête) pour pouvoir recueillir des informations à l'étranger.

En 2021, après analyse du cadre juridique pertinent, la VSSE et le SGRS ont été interrogés sur les éventuelles activités de renseignement qu'ils mènent à l'étranger. En raison d'autres priorités et de l'impact de la crise sanitaire sur les effectifs du Comité, le traitement de leurs réponses a été interrompu. L'enquête sera finalisée courant 2022.

---

171 Mais par exemple aussi : quelle est la signification/valeur de la notion d'État ami' dans le contexte des services de renseignement et dans quelle mesure cette notion détermine-t-elle la position de nos propres services de renseignement ?

I.14.7. CONTRÔLE DES FONDS SPÉCIAUX : ENQUÊTE DE SUIVI

À l'instar de tout service public, les services de renseignement se voient également allouer des fonds publics pour exercer leurs missions légales. La règle normale pour l'utilisation de ces fonds doit être une transparence parfaite et un contrôle total. Cependant, comme certaines tâches de la VSSE et du SGRS sont imprévisibles ou doivent être tenues secrètes, une partie de leur budget échappe à cette 'règle normale'. Cette partie est mieux connue sous le nom de 'fonds spéciaux'. Bien que le montant de ces fonds soit intégré dans le budget alloué aux services, des règles particulières s'appliquent à leur gestion, leur utilisation et leur contrôle. En 2015[172], le Comité s'est notamment attaché à déterminer la nature de ces 'fonds spéciaux', leur montant et leur répartition. Il a également contrôlé l'utilisation des moyens et les interactions entre ces 'fonds spéciaux' et les budgets dits 'normaux'. Enfin, le Comité s'est penché sur le cadre réglementaire et a examiné les mécanismes de contrôle, et ce tant en interne (au sein des services) qu'en externe (Cour des comptes, Inspection des Finances, Comité permanent R, etc.). Différentes recommandations ont été formulées.

Depuis 2018 (VSSE) et 2020 (SGRS), la Cour des comptes a exprimé son intention de réaliser un contrôle périodique de ces fonds. Dans ce contexte, la Cour des comptes a pu recourir à une assistance technique, telle que proposée par le Comité permanent R.[173] Le Comité pouvait à son tour « *exercer sa mission avec plus d'attention sur l'utilisation de ces dits fonds* ». Une enquête de suivi a été ouverte fin 2020 sur la gestion, l'utilisation et le contrôle des fonds spéciaux. Interrompus en raison de la prise en charge de dossiers prioritaires en 2021, les devoirs d'enquête reprendront en 2022.

172 COMITÉ PERMANENT R, *Rapport d'activités 2015*, 11-16 ('La gestion, l'utilisation et le contrôle des fonds spéciaux').

173 *« Ce contrôle sera périodique et comportera, outre un examen des processus et un contrôle de caisse, un contrôle formel réalisé par sondage et portant sur l'existence des pièces justificatives conformes aux instructions et approuvées par les fonctionnaires compétents. Le contrôle ne portera pas sur le bien-fondé ou la bonne gestion des opérations sous-jacentes et sera mis en œuvre, dans le respect des missions du SGRS, par des auditeurs disposant de l'habilitation de sécurité requise ».*

I.14.8. ENQUÊTE DE CONTRÔLE SUR LA DÉTECTION ET LE SUIVI PAR LES SERVICES DE RENSEIGNEMENT DES ORGANISATIONS PHILOSOPHIQUES A VISÉES POLITIQUES CONTRAIRES À L'ORDRE DÉMOCRATIQUE

En juillet 2021, le Comité permanent R a reçu la demande de la Présidente de la Chambre, d'ouvrir une enquête portant sur « *la manière dont les services de renseignement s'intéressent aux activités des mouvements sectaires à obédience religieuse ayant des visées politiques (autres mouvements salafistes politiques, Opus Dei, mouvement Civitas, etc.)* ».[174]

Cette demande fait suite à deux enquêtes réalisées par le Comité, à savoir l'enquête de contrôle sur la manière dont la Sûreté de l'État a assuré le suivi de la commissaire du gouvernement Ihsane Haouach[175] et l'enquête de contrôle relative au suivi par les services de renseignement de la mouvance des Frères musulmans.[176]

Fin 2021, après clarifications et en accord avec la Présidente de la Chambre, le spectre de l'enquête a été adapté. L'enquête sera réalisée en 2022.

174 Courrier du 19 juillet 2021 de la Présidente de la Chambre, E. TILLIEUX, au Président du Comité permanent R.

175 Voir 'I.11. Le suivi d'une commissaire du gouvernement par la VSSE' (*supra*).

176 Voir 'I.12. Une attention renouvelée pour les Frères musulmans' (*supra*).

CHAPITRE II.
LE CONTRÔLE DES MÉTHODES PARTICULIÈRES ET DE CERTAINES MÉTHODES ORDINAIRES DE RENSEIGNEMENT

Le Comité permanent R est tenu de faire preuve de transparence quant à l'utilisation des 'méthodes de recueil de données' (MRD) par les services de renseignement : l'article 35 §1, 1° de la Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (L.Contrôle) – tel que modifié par l'article 25 de la Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité (Loi MRD)[177] – précise que dans son rapport d'activités, le Comité « *consacre une attention spécifique aux méthodes spécifiques et exceptionnelles de recueil de données, telles qu'elles ont été visées dans l'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité […]* ». Par ailleurs, conformément à l'article 35 §2 L.Contrôle, le Comité doit faire annuellement rapport à la Chambre « *sur l'application de l'article 16/2 et de l'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité […].*[178] *Le rapport indique le nombre d'autorisations accordées, la durée des méthodes exceptionnelles de recueil de données, le nombre de personnes concernées et, le cas échéant, les résultats obtenus.*[179] *Il précise également les activités du Comité permanent R.* »

Le présent chapitre détaille les chiffres de la mise en œuvre par la Sûreté de l'État (VSSE) et par le Service Général du Renseignement et de la Sécurité (SGRS) des méthodes spécifiques et exceptionnelles (regroupées en 'méthodes particulières

177 Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité, *M.B.* 10 mars 2010.

178 Une copie de ce rapport est également adressée aux ministres de la Justice et de la Défense ainsi qu'à la Sûreté de l'État et au Service Général du Renseignement et de la Sécurité, qui ont la faculté d'attirer l'attention du Comité permanent R sur leurs observations (art.35 § 2 L.Contrôle).

179 Un rapport spécifique sur les 'résultats obtenus' n'est pas à l'ordre du jour pour l'instant. Le Comité est conscient qu'il s'agit d'une mission importante : *"there will be an important job for oversight bodies to measure the effectiveness of these new techniques while nonetheless providing public assurance that any new powers or resources are proportionate to the threat and not abused"*, in: I. LEIGH and N. WEGGE, *Intelligence oversight in the twenty-first century. Accountability in a changing world*, Routledge, 2020, 18.

de renseignement') ainsi que de certaines méthodes ordinaires, pour lesquelles le Comité s'est vu confier une mission de contrôle supplémentaire (lesdites 'méthodes ordinaires plus').

La manière dont le Comité a assuré sa mission de contrôle (juridictionnel) sur ces méthodes y est également présentée. Il y a plusieurs années, le Comité a fait le choix de publier sa jurisprudence dans les rapports d'activités annuels. Ces décisions, contenant pour certaines des éléments classifiés, ne sont pas publiées dans leur intégralité. Y sont mentionnés uniquement les éléments juridiques pertinents ainsi que les faits essentiels. Une telle transparence est (assez) unique. L'expérience des années passées a pu démontrer que pareille démarche est possible sans compromettre le fonctionnement des services de renseignement.

Notons également que le Comité peut être saisi en sa qualité d''auteur d'avis préjudiciels' (articles 131*bis*, 189*quater* et 279*bis* CIC).[180] Le cas échéant, le Comité rend un avis sur la légalité des méthodes spécifiques ou exceptionnelles ayant fourni des renseignements qui sont utilisés dans le cadre d'une affaire pénale. Jusqu'à présent, il s'agit d'un concept resté théorique, qui n'a donc pas été concrétisé au cours de la décennie écoulée.[181]

II.1. LES CHIFFRES RELATIFS AUX MÉTHODES PARTICULIÈRES ET À CERTAINES MÉTHODES ORDINAIRES

II.1.1. TENDANCES GÉNÉRALES

II.1.1.1. Quant aux méthodes particulières de renseignement à la VSSE et au SGRS

Le législateur a opté, à l'époque, pour une subdivision claire entre les différentes méthodes de recueil de données, désignées dans la loi comme méthodes ordinaires, spécifiques ou exceptionnelles. Elles sont (ou plutôt devraient être) classées selon leur degré d'ingérence (croissant) dans la vie privée et disposent chacune d'un cadre et d'un mécanisme de contrôle qui leur sont propres. La sévérité du contrôle

180 À ce propos, Voy. COMITÉ PERMANENT R, *Rapport d'activités 2010*, p.59.

181 La décision de demander un avis appartient aux juges d'instruction et aux juges pénaux. Au sujet de son application limitée, voir VANDERBORGHT, J., '*If you torture the data long enough, it will confess. Enkele cijfers over de inzet van bijzondere inlichtingenmethoden*', in VANDERBORGHT, J. (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers*, Intersentia, Antwerpen, 2020, 25.

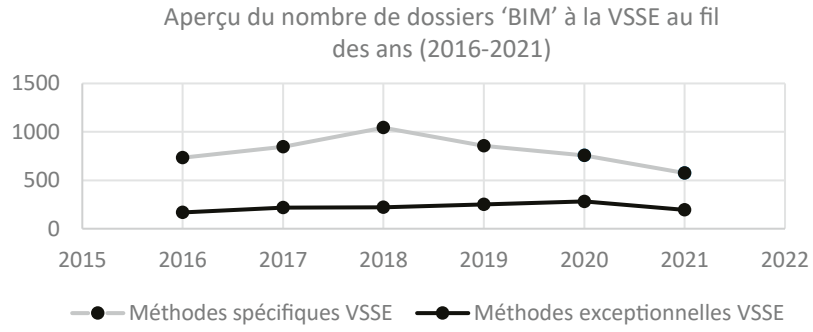
est proportionnelle au degré d'intrusion de la méthode utilisée.[182] L'objectif était d'éviter que les services recourent d'emblée aux mesures les plus lourdes.

Entre le 1er janvier et le 31 décembre 2021, 1823 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 1570 par la VSSE (1220 spécifiques et 350 exceptionnelles) et 253 par le SGRS (166 spécifiques et 87 exceptionnelles).[183]

---

182 De l'avis de certains experts, cette répartition semble trop théorique et ne tient pas suffisamment compte de la réalité. Voir par ex. W. VAN LAETHEM, 'Enkele reflecties over tien jaar BIM-controle door het Vast Comité I', in VANDERBORGHT, J. (ed.), *o.c.*, 70-72. Le Comité est du même avis et a cité, à titre d'exemples, les articles 16/3 L.R&S (collecte et traitement des données des passagers) et 16/4 L.R&S (collecte et traitement des images enregistrées par les caméras des services de police). Bien que ces pouvoirs d'investigation soient qualifiés de méthodes ordinaires, leur degré d'intrusion dans la vie privée et dans la protection des données est souvent plus important que certaines méthodes de renseignement spécifiques, voire exceptionnelles. C'est certainement le cas de l'utilisation des images caméras lorsque ce sont des caméras intelligentes ou des logiciels intelligents qui sont utilisés, tels que le système ANPR. Voir COMITÉ PERMANENT R, Avis n°001/CPR/2021 du 12 juillet 2021 (modifications Loi Renseignements), consultable sur www.comiteri.be. Les services de renseignement, pour leur part, soulignent la nécessité de maintenir le principe d'égalité avec les méthodes particulières de recherche.

183 Les services de renseignement s'appuient sur d'autres méthodes pour la comptabilisation. La VSSE calcule en nombre de dossiers 'BIM', un dossier pouvant contenir plusieurs méthodes. Une tendance similaire est néanmoins observée :

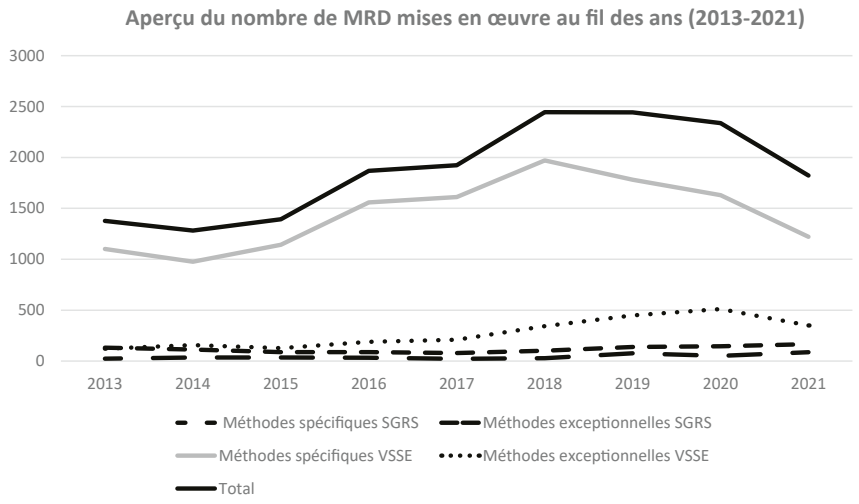


Le SGRS procède lui aussi d'une autre manière, puisqu'il comptabilise les méthodes par article sans subdivisions entre les différents paragraphes au sein d'un article comme le fait le Comité. Dans les chiffres du SGRS figurent également l'ensemble des demandes introduites en interne (même celles ayant fait l'objet d'un refus en interne). Enfin, une méthode est comptabilisée dans l'année où sa demande a été introduite, indépendamment de la date à laquelle elle a été autorisée.

Le tableau ci-dessous établit une comparaison avec les chiffres des années précédentes.

	SGRS		VSSE		TOTAL
	Méthodes spécifiques	Méthodes exceptionnelles	Méthodes spécifiques	Méthodes exceptionnelles	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868
2017	79	22	1612	210	1923
2018	102	28	1971	344	2445
2019	138	76	1781	449	2444
2020	146	51	1629	511	2337
2021	166	87	1220	350	1823

Cela donne schématiquement :



Après une augmentation constante du nombre de MRD mises en œuvre jusqu'en 2018 et une stagnation en 2019-2020, on remarque une diminution significative en 2021.[184] Une nuance s'impose car en divisant les chiffres par service, on constate pour 2021 une nette augmentation (environ 30 %) du nombre de MRD mises en œuvre par le SGRS. On note, à l'inverse, une nette diminution (environ 28 %) à la VSSE (*infra*).

[184] À noter que plusieurs *targets* (tels que des personnes, des organisations, des lieux, des objets, des moyens de communication, etc.) peuvent être visés dans une même autorisation.

Nonobstant un léger mouvement de rattrapage enregistré du côté du SGRS, la VSSE continue de se tailler la part du lion, avec 86 % des méthodes mises en œuvre. Bien que les deux services aient été dotés des mêmes compétences, leurs missions sont à ce point différentes (par exemple l'importance des missions du SGRS à l'étranger) que l'on ne peut guère tirer d'enseignements d'une comparaison entre les deux services. Une autre raison invoquée par les services pour expliquer ces différences, est notamment le fait que les MRD mises en œuvre par la Plateforme commune contre-terrorisme (Plateforme CT) concernant la menace terroriste sont comptabilisées dans les chiffres de la VSSE.

Une ventilation de ces chiffres permet de constater une poursuite de l'augmentation, constatée l'an dernier, du nombre de méthodes spécifiques mises en œuvre par le SGRS, passant de 146 à 166. Le nombre de méthodes exceptionnelles mises en œuvre connaît une forte augmentation, passant de 51 en 2020 à 87 en 2021.[185] Selon le SGRS, ce phénomène s'explique par la restructuration interne de la cellule BIM, qui implique une prestation de services plus efficace[186], et le recrutement de *case-managers* supplémentaires, avec pour conséquence davantage de '*request for operations*'. En termes de contenu, l'affaire Jürgen Conings (cf. *supra*) et les ramifications de ce dossier (extrême droite dans l'armée) ont eu un impact majeur. Mais abstraction faite de l'affaire précitée, une augmentation considérable du nombre de MRD mises en œuvre est encore constatée par le SGRS.

À la VSSE, on observe la tendance inverse, c'est-à-dire une diminution remarquable de l'utilisation des méthodes spécifiques (de 1629 en 2020 à 1220 en 2021) ainsi qu'une baisse de l'utilisation des méthodes exceptionnelles (de 511 en 2020 à 350 en 2021, soit une diminution de plus de 30 %). Selon le VSSE, plusieurs raisons expliquent cette tendance baissière : le nombre de méthodes dites « ordinaires plus » s'est inscrit à la hausse (principe des vases communicants) ; le service a connu un recrutement considérable, suivi d'une formation intensive accaparant de nombreuses forces vives et ayant impliqué une diminution du nombre d'agents disponibles pour les enquêtes ; les conséquences persistantes des mesures COVID, etc.

---

185 Ce qui est important à souligner dans ce contexte, c'est que le SGRS dispose également de compétences particulières pour le recueil d'informations, telles que réglées dans les articles 44 et suiv. L.R&S. Voir à ce propos 'Chapitre III. Le contrôle des interceptions à l'étranger, des prises d'images et des intrusions dans des systèmes informatiques'.

186 La procédure de soumission des MRD au SGRS resterait néanmoins sensiblement plus lourde (d'un point de vue administratif) qu'à la VSSE, ce qui donnerait lieu, selon le SGRS, à une forme d''autocensure'.

II.1.1.2. Quant aux méthodes ordinaires plus, en particulier l'article 16/2 L.R&S

L'identification de l'abonné ou de l'utilisateur habituel d'un service ou d'un moyen de télécommunication (par ex. le numéro de GSM ou l'adresse IP[187]) est considérée comme une méthode ordinaire, dans la mesure où elle est effectuée par une réquisition auprès des opérateurs ou des fournisseurs de télécommunication ou par un accès direct à leurs fichiers clients.[188] L'article prévoit l'obligation pour les services de renseignement de tenir un registre de toutes les identifications réquisitionnées et de toutes les identifications obtenues par accès direct.[189] Il stipule également que le Comité doit recevoir une liste mensuelle des identifications réquisitionnées et une liste de chaque accès.

En ce qui concerne cette méthode, la diminution déjà observée se poursuit. On dénombre une dizaine de réquisitions de moins au SGRS par rapport à 2020, et plus de 1000 réquisitions de moins du côté de la VSSE.[190]

	Réquisitions par le SGRS	Réquisitions par la VSSE
2016	216	2203
2017	257	4327
2018	502	6482
2019	442	5674
2020	433	5123
2021	420	4080

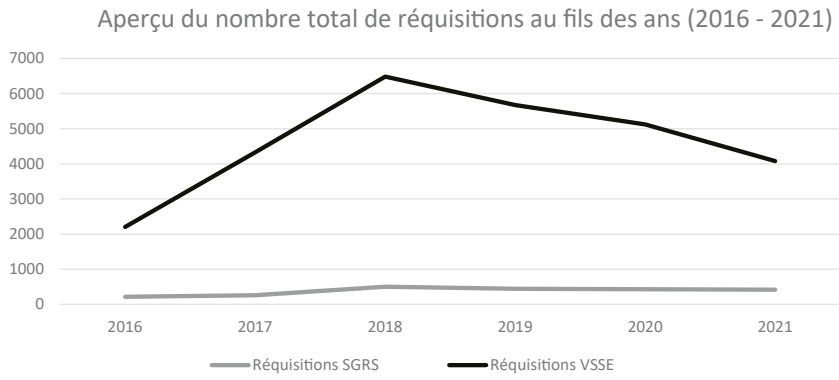
187 À compter de 2022, le nombre de réquisitions sera réparti entre les 'réquisitions IP' et les 'autres réquisitions'.

188 Lorsque l'identification est réalisée à l'aide d'un moyen technique (et donc pas via une réquisition auprès d'un opérateur) la collecte demeure une méthode spécifique (art. 18/7 § 1er L.R&S).

189 La possibilité offerte aux services de renseignement (par l'introduction du dernier alinéa de l'article 16/2 §1 L.R&S) de demander des identifications via un accès direct aux fichiers des clients d'un opérateur ou d'un fournisseur de télécommunications n'a pas encore été mise en œuvre.

190 Dans le cadre de son pouvoir général de contrôle, le Comité en a analysé les raisons. Les résultats ont été inclus dans l'"*enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R*" (cf. I.14.1. 'L'application de nouvelles méthodes (particulières) de renseignement').

Cela donne schématiquement :



Un certain nombre de commentaires importants s'imposent. On peut déduire du tableau ci-dessus qu'après la mise en œuvre des modifications de la loi en 2016 et 2017, le nombre de réquisitions a atteint un pic en 2018. Bien que le nombre de demandes soit une indication de la charge de travail, on ne peut rien en déduire concernant l'augmentation ou la diminution du nombre de 'sélecteurs' visés (numéros de téléphone, noms, adresses IP...). Alors que le nombre de réquisitions pour le service de renseignement militaire, par exemple, a diminué (de 433 en 2020 à 420 en 2021), le nombre de sélecteurs a remarquablement augmenté : de 5334 en 2020 à 6385 en 2021 (soit une augmentation de près de 20 %). Pour la VSSE, malgré la diminution du nombre de réquisitions, le nombre de sélecteurs est resté relativement stable (31.730[191] en 2021 contre 31.204 en 2020).

Par ailleurs, les deux services ne font aucune distinction dans le décompte entre l'article 16/2 § 1er L.R&S et l'article 16/2 § 2 L.R&S[192] (identification du titulaire d'une carte prépayée).

191 À la VSSE, le nombre d'identifications d'adresses IP était de 4 925 (3 188 en 2020). Les autres identifications s'élevaient à 26 805 (28 016 en 2020).

192 L'article 16/2 L.R&S stipule : '*§ 2 Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte prépayée visée dans l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, sur la base de la référence d'une transaction bancaire électronique qui est liée à la carte prépayée et qui a préalablement été communiquée par un opérateur ou un fournisseur en application du paragraphe 1er.*'

II.1.1.3. Les conséquences de l'annulation de la Loi sur la conservation des données ?[193]

Par son arrêt du 22 avril 2021, la Cour constitutionnelle a annulé la loi sur la conservation des données (loi *data retention*).[194] La Cour a jugé que la conservation généralisée et indifférenciée des données relatives aux communications électroniques viole le droit au respect de la vie privée et à la protection des données personnelles. Cet arrêt constitue un obstacle notamment pour les enquêtes de renseignement.

Il va sans dire que les données d'identification, de trafic et de localisation jouent un rôle important dans le travail de renseignement. C'est une des raisons pour lesquelles l'obligation de conservation des données a été créée à l'article 126 de la Loi relative aux communications électroniques (LCE).[195] Cet article imposait aux fournisseurs de services de téléphonie publique et aux opérateurs de réseaux publics de communications électroniques de conserver ces données pendant douze mois.[196]

Concrètement, la Cour constitutionnelle a jugé que la conservation des données doit désormais être l'exception ; la conservation ciblée des données doit toujours être proportionnée à l'objectif poursuivi.

Interrogés sur les implications de cet arrêt sur le fonctionnement des deux services de renseignement en 2021, tant le SGRS que la VSSE ont déclaré qu'elles étaient négligeables et qu'aucune conséquence majeure n'était observée à ce stade.

Entre-temps, le gouvernement a déposé un projet de loi qui vise essentiellement à rétablir un cadre juridique conforme à la jurisprudence en matière de conservation des « métadonnées » ou « données de trafic et de localisation » par les opérateurs.[197] Le gouvernement exprime le souhait que cette loi réparatrice entre en vigueur avant l'été 2022.[198]

---

193 Voir le chapitre VI.3. 'Avis relatif à la rétention des données'.

194 Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.* 18 juillet 2016. Communiqué de presse de la Cour constitutionnelle, "La Cour constitutionnelle annule l'obligation de la conservation généralisée et indifférenciée des données relatives aux communications électroniques", 22 avril 2021.

195 Loi du 13 juin 2005 relative aux communications électroniques, *M.B.* 20 mai 2005, 28070.

196 L'obligation de conservation de données vise non seulement le trafic téléphonique, mais aussi divers types de trafic Internet.

197 Projet de loi du 17 mars 2022 relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, *Doc. parl.*, Chambre, 2021-2022, n°55-2572/001.

198 Question de E. GILISSEN au ministre des Télécommunications relative à 'la loi sur la conservation des données' (*C.R.I.*, Chambre 2021-2022, 9 mars 2022, CRIV55 COM715, 11).

II.1.2. MÉTHODES UTILISÉES PAR LE SGRS

II.1.2.1. MÉTHODES ORDINAIRES 'PLUS'

Identification de l'abonné ou de l'utilisateur habituel de télécommunications

La diminution du nombre de réquisitions, précédemment observée, se poursuit. On dénombre une dizaine de réquisitions de moins au SGRS par rapport à 2020 (*supra*).

Accès aux données PNR

À côté de l'identification de l'abonné ou de l'utilisateur habituel de télécommunications comme méthode ordinaire plus, une loi a introduit début 2017,[199] la possibilité pour les services de renseignement d'avoir accès aux informations détenues par l'Unité d'information des passagers (BELPIU), et ce par le biais de recherches ciblées (art. 16/3 L.R&S et art. 27 de la Loi du 25 décembre 2016 relative au traitement des données des passagers (Loi PNR).[200] Le Comité est informé de l'utilisation de cette méthode et peut l'interdire le cas échéant.[201]

La réglementation PNR permet également de réaliser ce que l'on appelle une 'évaluation préalable', qui consiste à vérifier automatiquement la correspondance entre les données PNR et les listes ou fichiers de noms des services de renseignement et à envoyer des informations sur la base de '*hits*' validés (art. 24 Loi PNR). Le nombre de recherches effectuées dans les données PNR est resté stable en 2021 (28 en 2020, 29 en 2021). Plus de la moitié concernait des dossiers liés à la menace d'"espionnage".

Utilisation d'images enregistrées par les caméras des services de police

La Loi du 30 novembre 1998 organique des services de renseignement et de sécurité a été adaptée par la Loi du 21 mars 2018 (*M.B.* 16 avril 2018) pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des

199 Loi du 25 décembre 2016 (*M.B.* 25 janvier 2017).

200 La Cellule BIM du SGRS n'intervient pas ici ; la mise en œuvre s'opère via le membre du personnel du SGRS détaché au sein de BELPIU.

201 À l'inverse des méthodes reprises à l'article 16/2 L.R&S, il n'est pas prévu qu'un rapport doive être rédigé à l'intention du Parlement, l'article 35 § 2 L. Contrôle n'ayant pas été adapté. Suivant la suggestion émise par la Commission de suivi, le Comité a décidé de reprendre ces chiffres dans son rapport annuel et de ne pas attendre une éventuelle modification de la loi.

services de police. Une nouvelle méthode ordinaire a été introduite à cet effet (art. 16/4 §2 L.R&S).[202] [203]

Le SGRS a utilisé cette méthode en 2021 (pour la première fois) à quinze reprises. Trois des quinze demandes concernaient des demandes pour une période de moins d'un mois.

Les chiffres

Méthodes ordinaires plus (SGRS)	Nombre d'autorisations 2020	Nombre d'autorisations 2021
Identification de l'abonné ou de l'utilisateur habituel de télécommunications	433	420
Recherches ciblées de données PNR	28	29
Utilisation d'images enregistrées par les caméras des services de police[204]	Pas en vigueur	15

202 Cette même loi a étendu la possibilité d'observation spécifique et exceptionnelle existante (articles 18/4 § 3 et 18/11 § 3 L.R&S).

203 Début 2019, le Conseil des ministres a approuvé un projet d'arrêté royal en application de l'art. 16 § 4 L.R&S, qui a été soumis à l'avis du Comité permanent R. Cet avis 002/CPR-ACC/2019 du 9 avril 2019 peut être consulté sur le site internet du Comité (www.comiteri.be).

204 Le champ d'application de l'article 16/4 L.R&S (par ex. en ce qui concerne les consultations de la Direction de l'information policière et des moyens ICT (DRI) de la Police fédérale) fait l'objet d'une analyse juridique (2021).

II.1.2.2. Les méthodes spécifiques

Le tableau ci-dessous reprend les chiffres relatifs à l'application des méthodes spécifiques par le SGRS. On en distingue sept.

Méthodes spécifiques (SGRS)	Nombre d'autorisations 2020	Nombre d'autorisations 2021
Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 L.R&S)[205]	6	12
Inspecter des lieux accessibles au public, à l'aide d'un moyen technique, inspecter le contenu d'objets verrouillés ou les emporter (art. 18/5 L.R&S)	0	0
Prendre connaissance de données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art.18/6 L.R&S)	0	0
Requérir des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage (art. 18/6/1 L.R&S)	2	0
Identifier, à l'aide d'un moyen technique, les services et de moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée (art. 18/7 §1, 1° L.R&S)	2	6

[205] La Loi du 21 mars 2018 (*M.B.* 16 avril 2018) a ajouté un nouveau paragraphe à l'article 18/4 L.R&S pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services, et ce afin d'effectuer des observations en temps réel. Cette méthode, qui nécessite un accès direct aux informations visées, n'a pas encore été opérationnalisée.

Méthodes spécifiques (SGRS)	Nombre d'autorisations 2020	Nombre d'autorisations 2021
Requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, identifier le moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 §1, 2° L.R&S)	0	0
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 §1, 1°L.R&S)	69	75
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 §1, 2° L.R&S)	67	73
TOTAL	**146**	**166**

En ce qui concerne la mise en œuvre des méthodes spécifiques, ce sont le repérage des données d'appel d'un trafic de communications électroniques' (art. 18/8, §1, 1° L.R&S) et la 'prise de connaissance de données de localisation d'un trafic de communications électroniques' (art. 18/8, §1, 2° L.R&S), tous deux assortis d'une réquisition du concours d'un opérateur, qui se hissent distinctement en tête du classement (148 des 166 méthodes spécifiques mises en œuvre). Il y a deux fois plus d'observations dans des lieux accessibles au public à l'aide d'un moyen technique qu'en 2020, passant de 6 en 2020 à 12 en 2021.

Selon le SGRS, un certain nombre de méthodes n'ont pas été utilisées en raison d'un manque de personnel. Il a par ailleurs été constaté par le SGRS qu'un certain nombre de méthodes spécifiques n'étaient pas suffisamment connues du personnel et, par conséquent, pas assez utilisées. Pour y remédier, des briefings internes ont été organisés début 2022.

II.1.2.3. Les méthodes exceptionnelles

Dans le cadre de ses missions visées aux articles 11, § 1er, 1° à 3° en 5°, et § 2 L.R&S, le SGRS peut mettre en œuvre différentes méthodes exceptionnelles :

Méthodes exceptionnelles (SGRS)	Nombre d'autorisations 2020	Nombre d'autorisations 2021
Observer, à l'aide ou non de moyens techniques, des lieux non accessibles au public qui sont soustraits à la vue et pénétrer dans des lieux non accessibles au public qui sont soustraits ou non à la vue pour exécuter une observation, installer un moyen technique, ouvrir un objet ou l'emporter (art. 18/11 L.R&S)[206]	2	3
Inspecter, à l'aide ou non de moyens techniques, des lieux non accessibles au public, ainsi que l'inspection du contenu d'objets verrouillés ou non qui s'y trouvent (art. 18/12 L.R&S)	0	2
Recourir à une personne morale visée à l'article 18/3, § 1er L.R&S afin de collecter des données	0	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	0	2
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	6	8
S'introduire dans un système informatique (article 18/16 L.R&S)	4	14
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	39	60
TOTAL	**51**	**89**

Comme indiqué, une forte augmentation du nombre de méthodes exceptionnelles mises en œuvre est constatée. La forte augmentation en pourcentage (quasi un doublement) du nombre de méthodes exceptionnelles mises en œuvre par le SGRS s'explique principalement par l'augmentation du nombre d'intrusions dans un système informatique (18/16 L.R&S) (passant de 4 en 2020 à 14 en 2021) et du nombre d'interceptions, de prises de connaissance et d'enregistrements de communications (art. 18/17 L.R&S) (de 39 en 2020 à 60 en 2021). La méthode exceptionnelle consistant à recourir à une personne morale afin de collecter des

[206] La Loi du 21 mars 2018 (*M.B.* 16 avril 2018) a ajouté un nouveau paragraphe à l'article 18/11 L.R&S pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services, et ce afin d'effectuer des observations en temps réel. Cette méthode, qui nécessite un accès direct aux informations visées, n'a pas encore été opérationnalisée.

données (art. 18/13 L.R&S) n'a encore jamais été utilisée par le SGRS, et ce depuis l'entrée en vigueur de la loi de 2010. En 2016, le même constat était déjà posé et expliqué par le fait que « *la procédure de création est trop lourde pour la mettre en œuvre pour un seul dossier* ».[207] Le Comité rappelait[208] au SGRS l'obligation d'informer la Commission BIM toutes les deux semaines de la mise en œuvre de ces méthodes exceptionnelles (art. 18/10 § 1er, alinéa 3 L.R&S et art. 9 AR 12 octobre 2010). À cette fin, une réunion dite 'de quinzaine' a été mise en place. Les mesures sanitaires imposées dans le cadre de la crise du coronavirus ont empêché la tenue de ces réunions. Elles ont repris au printemps 2022.

II.1.2.4. Les missions et les menaces justifiant le recours aux méthodes ordinaires et particulières[209]

Le SGRS est autorisé à employer les méthodes spécifiques et exceptionnelles dans le cadre de quatre missions[210] suivants différentes menaces.

1. **La mission de renseignement (art. 11, 1° L.R&S)**
   Le recueil, l'analyse et le traitement du renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir. Le recueil, l'analyse et le traitement du renseignement relatif à toute activité qui menace ou pourrait menacer les intérêts suivants :
   - l'intégrité du territoire national ou la survie de tout ou partie de la population ;
   - les plans de défense militaires ;
   - le potentiel économique et scientifique en rapport avec la défense ;
   - l'accomplissement des missions des Forces armées ;
   - la sécurité des ressortissants belges à l'étranger.
2. **Veiller au maintien de la sécurité militaire (art. 11, 2° L.R&S)**
   - la sécurité militaire du personnel relevant du ministre de la Défense nationale ;

---

207 Exposé des motifs du projet de loi modifiant la loi du 30 novembre 1998, *Doc. Parl.*, Chambre, 2015-2016, n°54-2043/001, 11.

208 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 109, ('XII.II.3.3. Obligation d'information dans le cadre des méthodes exceptionnelles').

209 Plusieurs intérêts et menaces peuvent figurer dans une même autorisation.

210 Ces méthodes ne peuvent donc pas être utilisées dans le cadre d'enquêtes de sécurité ou d'autres missions assignées au SGRS par ou conformément à des lois particulières (par ex. effectuer des vérifications de sécurité pour des candidats militaires)

- les installations militaires, armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires ;
- dans le cadre des cyberattaques de systèmes informatiques et de communications militaires ou de ceux que le ministre de la Défense nationale gère, neutraliser l'attaque et en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés.

3. **La protection de secrets (art. 11, 3° L.R&S)**
   La protection du secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national et l'accomplissement des missions des Forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que gère le ministre de la Défense nationale.
4. **La recherche, l'analyse et le traitement du renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge (art. 11, 5°, L.R&S).**

Depuis l'entrée en vigueur de la Loi du 30 mars 2017, la mise en œuvre de méthodes particulières n'est plus limitée au territoire belge (art. 18/1, 2° L.R&S). Le SGRS a fait savoir qu'aucune MRD n'avait été mise en œuvre à l'étranger en 2021.[211] Cette compétence, qui n'a pas encore été exercée, avait pourtant été présentée, dans l'exposé des motifs de la Loi du 30 mars 2017, comme une nécessité pour permettre au SGRS de mener à bien ses missions à l'étranger (notamment celles exécutées dans le cadre des opérations avec mandat donné par le Conseil de Sécurité des Nations Unies).[212] Une enquête plus approfondie devrait permettre d'établir si le SGRS n'a effectivement jamais eu recours à des MRD à l'étranger depuis l'entrée en vigueur de cette loi – ce qui reviendrait à contredire l'argumentaire développé dans l'exposé des motifs – ou si des MRD ont été mises en œuvre à l'étranger sans recours à la procédure MRD qui s'impose pourtant. Le Comité vérifiera en 2022 si le SGRS a fait usage (à tort ?) exclusivement du régime décrit à l'article 44 (voir chapitre III 'Le contrôle des interceptions à l'étranger, des prises d'images et des intrusions dans les systèmes informatiques').[213]

---

211 Il a par contre été fait recours aux possibilités offertes à l'article 44 L.R&S. (Voir à ce propos le chapitre III 'Le contrôle des interceptions à l'étranger, des prises d'images et des intrusions dans les systèmes informatiques').

212 Exposé des motifs, *Doc. Parl.*, Chambre 2015-2016, n°54-2043/001.

213 Cette initiative s'inscrit d'ailleurs dans la logique de la loi de 2017 dont l'exposé des motifs indiquait *« dans cinq ans, il sera procédé à une nouvelle évaluation de la situation pour voir si les prérogatives en faveur du SGRS sont praticables à l'étranger et si elles couvrent suffisamment les mandats des Nations Unies »*.

Aucune méthode particulière de renseignement n'a par ailleurs été mise en œuvre à la demande d'un service partenaire étranger.[214] Par contre, comme le précise le SGRS, les informations obtenues d'un service étranger peuvent être à la source de la mise en œuvre d'une MRD.

La pratique a montré que plusieurs menaces peuvent figurer dans une même autorisation. Une légère baisse peut être observée dans la mise en œuvre des MDR pour les menaces 'espionnage' et 'terrorisme'. Il convient de noter la forte augmentation du nombre de méthodes exceptionnelles mises en œuvre dans le cadre de la menace 'extrémisme' (de 20 en 2020 à 82 en 2021). Il n'est pas surprenant que cette forte augmentation soit due à l'affaire Jürgen Conings[215] et à l'attention particulière portée à l'extrême droite au sein des Forces armées qui en a résulté. Pour la première fois, les 'organisations criminelles' sont également mentionnées comme une menace (29 méthodes utilisées).[216]

NATURE DE LA MENACE	NOMBRE EN 2020	NOMBRE EN 2021
Espionnage	139	120
Ingérence	19	16
Extrémisme	20	82
Terrorisme	19	9
Organisations criminelles	-	26
Autre	-	0
Total	**197**	**253**

Contrairement à la mise en œuvre de méthodes particulières, le Comité ne dispose pas de données chiffrées relatives à la menace visée et aux intérêts à défendre en ce qui concerne les méthodes ordinaires dont il est question dans le présent chapitre. Dans son précédent rapport d'activités, le Comité recommandait aux services de consigner ces données et de les tenir à disposition.[217] Étant donné que ce n'est pas encore le cas, le Comité réitère sa recommandation.

214 Cela semblait être le cas pour la mise en œuvre de mesures 'ordinaires plus' (mais uniquement dans la mesure où cela représente également un intérêt manifeste pour le SGRS lui-même et que cela entre dans son champ de compétence).

215 Voir 'I.9. Enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings'

216 Deux dossiers spécifiques semblent l'expliquer : l'un relatif au trafic d'armes/crime organisé et l'autre relatif au trafic de drogue (initialement ouvert dans le cadre du suivi de l'extrême droite).

217 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 43.

II.1.3. LES MÉTHODES UTILISÉES PAR LA VSSE

II.1.3.1. Les méthodes ordinaires 'plus'

Méthodes ordinaires plus (VSSE)	Nombre d'autorisations en 2020	Nombre d'autorisations en 2021
Identification de l'abonné ou de l'utilisateur habituel de télécommunications	5123	4080
Recherches ciblées de données PNR[218]	30	98[219]
Utilisation d'images enregistrées par les caméras des services de police	Pas en vigueur	

En ce qui concerne les « méthodes ordinaires plus », on constate pour la troisième année consécutive une forte diminution (+/-1000 identifications demandées) du nombre d'' identifications de l'abonné ou de l'utilisateur habituel de télécommunications'.[220] En revanche, le recours aux méthodes fondées sur les articles 16/3 et 16/4 L.R&S est en augmentation constante. Le nombre d'autorisations de recherches ciblées dans les données des passagers (PNR) (Art. 16/3 L.R&S) a plus que triplé (de 30 à 98). L'utilité de cette méthode ne cesse de croître compte tenu de l'augmentation exponentielle du nombre de compagnies aériennes intégrées au système.[221] Depuis 2021, l'art. 16/4 §2 L.R&S, régissant la demande de consultation par les services de renseignement des images préalablement enregistrées des caméras de police, peut également être invoqué.[222] Les exigences procédurales s'appliquent à la fois aux récupérations ciblées d'images de caméras de police par un accès direct (en ligne) aux bases de données policières pertinentes (ce qui n'est

---

218 Le profilage n'est pas (encore) utilisé.

219 Le rapport d'activités de BELPIU indique qu'en 2021 « *la VSSE a introduit 133 demandes de recherches dans le passé* », Centre de crise national, *Rapport annuel BELPIU 2021*, 14.

220 Dans la pratique, c'est le '*common reference database center*' (CRDC) qui est consulté en premier lieu. Cette base de données fournit exclusivement de l'information sur l'opérateur assurant le service du numéro demandé, sans mentionner si ce numéro a été attribué à un utilisateur final. Aucune donnée à caractère personnel n'est conservée dans cette 'banque de données de localisation de numéro accessible au public'.

221 "*Le nombre de données passagers traitées en 2021 a été plus faible qu'en 2019. En revanche, davantage de données ont été traitées qu'en 2020, car l'unité traite les données relatives aux passagers d'un plus grand nombre de compagnies aériennes. Actuellement, les données de 94 % du trafic aérien international sont traitées. En outre, au sein de la BelPIU, les données relatives aux passagers sont traitées de manière plus ciblée et les collaborations avec d'autres unités européennes d'information sur les passagers (PIU) sont plus nombreuses*", dans : Rapport annuel BELPIU 2021.

222 Début 2022, le Comité permanent R, en sa qualité d'autorité de contrôle, a rendu une décision à ce propos : COMITÉ PERMANENT R, décision APD n° VCI-DPA/2022/2 – Instruction de traitement concernant la récupération rétroactive d'images de caméras de police par les services de renseignement sur la base de l'article 16/4, §2 L.R&S.

pas possible pour le moment) et aux récupérations ciblées par une demande écrite adressée aux services de police compétents[223] (en l'occurrence, la Direction de l'information policière et des moyens ICT de la Police fédérale (DRI)). La méthode a été utilisée à 46[224] reprises.

L'identification des titulaires des cartes prépayées n'est pas comptabilisée comme une méthode séparée.

II.1.3.2. Les méthodes spécifiques

Méthodes spécifiques (VSSE)	Nombre d'autorisations en 2020	Nombre d'autorisations en 2021
Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 L.R&S)	245	195
Inspecter des lieux accessibles au public, à l'aide d'un moyen technique, inspecter le contenu d'objets verrouillés ou les emporter (art. 18/5 L.R&S)	0	0
Prendre connaissance de données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art.18/6 L.R&S)	1	0
Requérir des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage (art. 18/6/1 L.R&S)	70	33

[223] Depuis l'entrée en vigueur de la Loi caméras du 21 mars 2018, les demandes écrites d'images de caméras de police doivent être fondées sur la base de l'article 16/4, §2 L.R&S. Les services de renseignement ne peuvent plus utiliser l'article 14, alinéa 2 L.R&S à cette fin. Voir à cet égard la décision-APD n° VCI-DPA/2022/2 (*supra*).

[224] En 2021, seules les méthodes dépassant le délai d'un mois ont été mentionnées. Dans sa décision n° VCI-DPA/2022/2, le Comité a souligné que « *les demandes écrites de DRI ne peuvent avoir lieu qu'en respectant les deux exigences procédurales mentionnées ci-dessus (confirmation écrite et notification), et ce indépendamment du fait que l'accès aux données des caméras de police ait lieu pendant ou après le premier mois de conservation* » .

Méthodes spécifiques (VSSE)	Nombre d'autorisations en 2020	Nombre d'autorisations en 2021
Identifier, à l'aide d'un moyen technique, les services et de moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée (art. 18/7 §1, 1° L.R&S)	46	22
Requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, identifier le moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 §1, 2° L.R&S)	0	2
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S)	650	491
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S)	617	477
TOTAL	**1629**	**1220**

Le nombre de méthodes spécifiques mises en œuvre a de nouveau nettement diminué (1629 à 1220). Pour pratiquement toutes les méthodes spécifiques, une diminution est observée. En plus des raisons générales mentionnées ci-dessus (nouveaux recrutements, mesures prises dans le cadre de la crise sanitaire), il y a selon la VSSE plusieurs éléments qui peuvent l'expliquer. Par exemple, l'utilisation de la méthode spécifique régie par l'article 18/6/1 L.R&S (la réquisition de données de transport ou de voyage) semble être liée aux recherches PNR ; étant donné l'augmentation du nombre de recherches ciblées dans les données PNR, l'utilisation de cette méthode spécifique a diminué (principe des vases communicants).[225] En ce qui concerne les inspections dans les lieux accessibles au public (art. 18/5 L.R&S) et la prise de connaissance des données d'identification du courrier postal

[225] Pour les données des compagnies aériennes qui ne sont pas (encore) intégrées dans BELPIU, les demandes sont encore effectuées sur la base de l'article 18/6/1 L.R&S. La VSSE souhaite pouvoir, à l'avenir, interroger également l'économie collaborative (Uber, trottinettes partagées) dans ce cadre.

(art. 18/6 L.R&S)[226], la VSSE préfère, comme en 2020, l'utilisation d'une méthode exceptionnelle afin de s'assurer d'opérer dans le respect du cadre légal.

II.1.3.3. Les méthodes exceptionnelles

Méthodes exceptionnelles (VSSE)	Nombre d'autorisations en 2020	Nombre d'autorisations en 2021
Observer, à l'aide ou non de moyens techniques, des lieux non accessibles au public qui sont soustraits à la vue et pénétrer dans des lieux non accessibles au public qui sont soustraits ou non à la vue pour exécuter une observation, installer un moyen technique, ouvrir un objet ou l'emporter (art. 18/11 L.R&S)	9	13
Inspecter, à l'aide ou non de moyens techniques, des lieux non accessibles au public, ainsi que l'inspection du contenu d'objets verrouillés ou non qui s'y trouvent (art. 18/12 L.R&S)	8	11
Recourir à une personne morale visée à l'article 13/3, § 1er L.R&S afin de collecter des données	0	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	11	13
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	186	73
S'introduire dans un système informatique (article 18/16 L.R&S)	74	61
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	223	192
TOTAL	**511**	**363**

Comme pour les méthodes spécifiques, le nombre de méthodes exceptionnelles mises en œuvre par la VSSE est en diminution (de 511 en 2020 à 363 en 2021). Cette forte baisse s'explique presque entièrement par une réduction de moitié de l'utilisation de la méthode 'Collecte des données concernant des comptes bancaires et des transactions bancaires' (art. 18/15 L.R&S), passant de 186 en 2020 à 73 en

[226] Au regard des informations réceptionnées concernant l'envoi postal, il est plus indiqué d'introduire une demande de méthode exceptionnelle.

2021. Il s'avère que la mise en œuvre de cette méthode (le traitement de données financières) nécessite un travail particulièrement intensif.[227] On observe par ailleurs une légère diminution du nombre de méthodes utilisées pour l'écoute, la prise de connaissance et l'enregistrement des communications (art. 18/17 L.R&S) (de 223 en 2020 à 192 en 2021). Selon la VSSE, le recours à une personne morale (art. 18/13 L.R&S) requiert également trop de moyens.

II.1.3.4. Les menaces et les intérêts justifiant le recours aux méthodes (ordinaires et) particulières

Le tableau suivant reprend les menaces (potentielles) dans le cadre desquelles la VSSE a mis en œuvre des méthodes spécifiques et exceptionnelles. Une méthode peut naturellement viser plusieurs menaces. La VSSE peut utiliser les méthodes spécifiques dans le cadre de toutes les menaces qui entrent dans ses compétences (art. 8 L.R&S).

En considérant que plusieurs menaces peuvent figurer dans une même autorisation, les chiffres sont les suivants :

NATURE DE LA MENACE	NOMBRE EN 2020	NOMBRE EN 2021
Espionnage	816	478
Ingérence	27	121
Extrémisme	296	279
Prolifération	3	2
Organisations sectaires nuisibles	0	0
Terrorisme	998	690
Organisations criminelles	0	0
Suivi des activités des services étrangers en Belgique	(inclus dans les chiffres ci-dessus)	(inclus dans les chiffres ci-dessus)
TOTAL	**2140**	**1570**

Le tableau repris ci-dessus montre pour ce qui est de la mise en œuvre de MRD en 2021 que la menace 'terrorisme' – bien qu'une diminution soit observée (de 998 à 690) – demeure la priorité absolue de la VSSE suivie par la menace 'espionnage'.

---

[227] L'avant-projet de loi 'modifiant la loi organique des services de renseignements', pour lequel le Comité a rendu un avis en 2021, propose d'introduire, à cet égard, une nouvelle méthode ordinaire. Il propose de créer une obligation pour les institutions financières, au sens large du terme, de coopérer afin d'identifier les produits ou services financiers dont dispose une personne ou, inversement, d'identifier quelle personne peut être liée à certains produits ou services financiers. Dans l'exposé des motifs, ce choix est justifié par le fait que « *le caractère intrusif d'une telle méthode […] faible à très faible* ». Le Comité ne partage pas cet avis. Dans son avis n°001/CPR/2021 du 12 juillet 2021 – modifications Loi Renseignement, il a recommandé de considérer cette méthode comme une méthode spécifique.

Alors qu'en 2020, il était question d'une forte diminution du nombre de dossiers 'ingérence', on relève à nouveau une importante augmentation (de 27 en 2020 à 121 en 2021). Dans la pratique, il n'est cependant pas toujours évident d'établir une distinction entre l'espionnage (recueillir clandestinement des données) et l'ingérence (influencer des processus décisionnels). La menace 'extrémisme-radicalisme' est restée stable (279 dossiers). Étant donné que les organisations sectaires nuisibles et les organisations criminelles ne font plus l'objet d'un suivi actif depuis 2015[228], ces menaces, sans surprise, ne figurent pas dans les chiffres.

En termes de territorialité, la VSSE est compétente pour mettre œuvre des MRD 'sur et à partir du territoire belge' (art.18/1, 1° L.R&S). À l'instar du SGRS, la VSSE n'a pas mis en œuvre de MRD à l'étranger. Le nombre de MRD mises en œuvre en Belgique à la demande de services partenaires étrangers est également négligeable. La mise en œuvre de certaines MRD a néanmoins été décidée sur la base d'informations obtenues de services partenaires.

La compétence de la VSSE n'est pas seulement définie par la nature de la menace. Le service n'est autorisé à intervenir que pour la sauvegarde d'intérêts bien déterminés :

1. La sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, c'est-à-dire :
   a) la sécurité des institutions de l'État et la sauvegarde de la continuité du fonctionnement régulier de l'État de droit, des institutions démocratiques, des principes élémentaires propres à tout État de droit, ainsi que des droits de l'homme et des libertés fondamentales ;
   b) la sécurité et la sauvegarde physique et morale des personnes et la sécurité et la sauvegarde des biens.
2. La sûreté extérieure de l'État et les relations internationales : la sauvegarde de l'intégrité du territoire national, de la souveraineté et de l'indépendance de l'État, des intérêts des pays avec lesquels la Belgique poursuit des objectifs communs, ainsi que des relations internationales et autres que la Belgique entretient avec des États étrangers et des institutions internationales ou supranationales.
3. La sauvegarde des éléments essentiels du potentiel économique et scientifique.

Comme le SGRS, la VSSE combine plusieurs intérêts. On peut néanmoins mentionner que la 'sauvegarde des éléments essentiels du potentiel économique et scientifique' est un intérêt qui mobilise peu.

Pour rappel, le Comité ne dispose pas des chiffres relatifs à la menace visée et aux intérêts à défendre en ce qui concerne les méthodes ordinaires dont il est question dans le présent chapitre.

---

228 Voir à ce propos, 'I.5. Le suivi des organisations sectaires nuisibles et des organisations criminelles par la Sûreté de l'État'.

II.2. LES ACTIVITÉS DU COMITÉ PERMANENT R EN SA QUALITÉ D'ORGANE (JURIDICTIONNEL) ET D'AUTEUR D'AVIS PRÉJUDICIELS

II.2.1. CONTRÔLE DE CERTAINES MÉTHODES ORDINAIRES

II.2.1.1. Généralités

Le contrôle de certaines méthodes ordinaires est réglementé différemment pour chacune de ces méthodes.

En ce qui concerne l'identification de l'utilisateur de télécommunications (et l'identification de l'utilisateur d'une carte prépayée qui y est associée), la loi n'a pas instauré de contrôle spécifique. À l'article 16/2 § 4 L.R&S, il est stipulé uniquement que la liste des identifications requises et de tous les accès directs doit être communiquée chaque mois au Comité. Comme déjà mentionné, le Comité reçoit uniquement le nombre de réquisitions. Il a toutefois proposé de contrôler annuellement une sélection de réquisitions.[229]

En ce qui concerne l'accès aux données PNR, qui sont détenues par l'Unité d'information des passagers, l'article 16/3 L.R&S dispose que c'est le dirigeant du service qui doit décider de tout accès, et ce '*de façon dûment motivée*'. Le Comité doit en être informé *et* '*interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les conditions qui ne respectent pas les conditions légales*'. Le Comité a prononcé quatre interdictions de ce type en 2021. Trois décisions de la VSSE ainsi qu'une décision du SGRS ne répondaient en effet pas pleinement à l'obligation légale de motivation. Dans le cadre de ces dossiers, les deux services ont été interdits d'exploiter les données recueillies.

Enfin, le Comité s'est vu attribuer des modalités de contrôle particulières dans le cadre de la possibilité pour les services de renseignement d'avoir accès à des informations provenant d'images enregistrées par des caméras utilisées par les

---

229 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 25, note de bas de page 41. Ce contrôle a débuté en 2020. Le Comité a décidé de reprendre cette thématique dans l'enquête qu'il a initiée en 2019 et qui est intitulée *'enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R.'*

services de police (article 16/4 L.R&S): un contrôle *a priori* [230] et un contrôle *a posteriori*.[231]

II.2.2. CONTRÔLE DES MÉTHODES PARTICULIÈRES

II.2.2.1. Les chiffres

Cette section reprend les activités du Comité permanent R relatives aux méthodes de renseignement spécifiques et exceptionnelles. L'attention se focalise ici sur les décisions juridictionnelles prises en la matière, et non sur les données opérationnelles. Il convient toutefois de souligner au préalable que le Comité soumet *toutes* les autorisations de mise en œuvre de méthodes particulières à une enquête *prima facie*, et ce en vue de décider d'une éventuelle saisine. Avant le début des mesures covid, un commissaire-auditeur du service d'Enquêtes participait aux réunions de quinzaine, au cours desquelles la VSSE informe la Commission BIM sur l'exécution des méthodes exceptionnelles. Pour des raisons évidentes, ces réunions ont été suspendues. Comme mentionné ci-dessus, ce type d'initiative reprendra au printemps 2022.

L'article 43/4 L.R&S stipule que le Comité permanent R peut être saisi de cinq manières :

1. D'initiative ;
2. À la demande de l'Autorité de protection des données (APD);
3. Par le dépôt d'une plainte d'un citoyen ;
4. De plein droit, chaque fois que la Commission BIM a suspendu une méthode spécifique ou exceptionnelle pour cause d'illégalité et a interdit l'exploitation des données ;
5. De plein droit, quand le ministre compétent a donné son autorisation sur base de l'article 18/10, § 3 L.R&S.

Par ailleurs, le Comité peut aussi être saisi en sa qualité d'ʻauteur d'avis préjudiciels' (articles 131*bis*, 189*quater* et 279*bis* CIC). Le cas échéant, le Comité rend un avis sur la légalité des méthodes spécifiques ou exceptionnelles ayant fourni des

---

230 '*Les critères d'évaluation visés à l'alinéa 1er, 2°, sont préalablement présentés au Comité permanent R.*'

231 '*La décision du dirigeant du service ou de son délégué et sa motivation sont transmises au Comité permanent R dans les meilleurs délais. La décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique. Dans ce cas, une liste des accès ponctuels est communiquée une fois par mois au Comité permanent R. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les conditions qui ne respectent pas les conditions légales*' et '*Chaque liste avec laquelle la corrélation visée à l'alinéa 1er, 1°, est réalisée, est communiquée dans les meilleurs délais au Comité permanent R. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les circonstances qui ne respectent pas les conditions légales.*'

renseignements qui sont utilisés dans le cadre d'une affaire pénale. Les demandes d'avis sont introduites par les juridictions d'instruction ou par les juridictions de fond. Le Comité n'intervient pas alors *stricto sensu* comme un organe juridictionnel.

TYPE DE SAISINE	2013	2014	2015	2016	2017	2018	2019	2020	2021
1. D'initiative	16	12	16	3	1	1	4	2	1
2. Commission Vie Privée/ Autorité de protection des données	0	0	0	0	0	0	0	0	0
3. Plainte	0	0	0	1	0	0	0	0	0
4. Interdiction d'exploitation par la Commission BIM[232]	5	5	11	19	15	10	12	9	8
5. Autorisation du ministre	2	1	0	0	0	0	0	0	0
6. Auteur d'avis préjudiciel	0	0	0	0	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**	**11**	**9**

Le nombre de décisions prises par le Comité a continué à diminuer (de 11 en 2020 à 9 en 2021). En outre, toutes les saisines, à une exception près, résultent d'une suspension décidée par la Commission BIM. Le Comité n'a encore jamais été saisi par l'Autorité de protection des données ou par un citoyen.

Une fois saisi, le Comité peut prendre plusieurs types de décisions et de décisions intermédiaires.

1. Constater la nullité de la plainte pour cause de vice de forme ou absence d'un intérêt personnel et légitime (art. 43/4, alinéa 1er, L.R&S) ;
2. Ne pas donner suite à une plainte qui est manifestement non fondée (art. 43/4, alinéa 1er, L.R&S) ;
3. Suspendre la méthode contestée dans l'attente d'une décision définitive (art. 43/4, dernier alinéa, L.R&S) ;
4. Demander des informations complémentaires à la Commission BIM (43/5 § 1er, alinéa 1er à 3, L.R&S) ;
5. Demander des informations complémentaires au service de renseignement concerné (43/5 § 1er, alinéa 3, L.R&S) ;
6. Ordonner une mission d'enquête pour le service d'Enquêtes R (art. 43/5 § 2 L.R&S). Dans cette rubrique, il est fait référence à la fois aux multiples

[232] Elles découlent, par exemple, de problèmes d'enregistrement ou d'enlèvement d'appareillages.

informations complémentaires recueillies de manière plutôt informelle par le Service d'Enquêtes R avant la saisine proprement dite et aux informations recueillies par le Comité après la saisine ;

7. Procéder à l'audition des membres de la Commission BIM (art. 43/5 § 4, alinéa 1er, L.R&S) ;
8. Procéder à l'audition du dirigeant du service de renseignement ou des membres du service de renseignement concerné (art. 43/5 § 4, alinéa 1er, L.R&S) ;
9. Statuer sur les secrets relatifs à une information ou à une instruction judiciaire en cours dont les membres des services de renseignement sont dépositaires, après concertation avec le magistrat compétent (art. 43/5 § 4, alinéa 2, L.R&S) ;
10. Pour le président du Comité permanent R, statuer, après avoir entendu le dirigeant du service, si le membre du service de renseignement estime devoir garder le secret dont il est dépositaire parce que sa divulgation est de nature à porter préjudice à la protection des sources, à la protection de la vie privée de tiers ou à l'accomplissement des missions du service de renseignement (art. 43/5 § 4, alinéa 3, L.R&S ;
11. Mettre fin à la méthode concernée si celle-ci est toujours en cours ou si elle a été suspendue par la Commission BIM, et interdire l'exploitation des données recueillies grâce à cette méthode et leur destruction (art. 43/6 § 1er, alinéa 1er, L.R&S) ;
12. Mettre fin partiellement à une méthode autorisée. Il est question ici, par exemple, d'une situation où une méthode est limitée dans le temps, pas d'une situation où une seule autorisation d'un dirigeant du service autorise plusieurs méthodes et où le Comité ne met fin qu'à une seule d'entre elles ;
13. Lever totalement ou partiellement la suspension et l'interdiction qui ont été décidées par la Commission BIM (art. 43/6 § 1er, alinéa 1er, L.R&S). Ceci implique que la méthode autorisée par le dirigeant du service soit (partiellement) considérée comme légale, proportionnelle et subsidiaire par le Comité ;
14. Constater l'incompétence du Comité permanent R ;
15. Déclarer le caractère infondé de l'affaire pendante et permettre la poursuite de la méthode ;
16. Délivrer un 'avis préjudiciel' (art. 131*bis*, 189*quater* et 279*bis* CIC).

NATURE DE LA DÉCISION	2014	2015	2016	2017	2018	2019	2020	2021
Décisions préalables à la saisine								
1. Plainte frappée de nullité	0	0	0	0	0	0	0	0
2. Plainte manifestement non fondée	0	0	0	0	0	0	0	0
Décisions intermédiaires								
3. Suspension de la méthode	3	2	1	0	0	0	1	0
4. Information complémentaire de la Commission BIM	0	0	0	0	0	0	0	0
5. Information complémentaire du service de renseignement	1	1	4	0	0	0	1	1
6. Mission d'enquête confiée au Service d'Enquêtes R[233]	54	48	60	35	52	52	24	33
7. Audition membres de la Commission BIM	0	2	0	0	0	0	0	0
8.Audition membres des services de renseignement	0	2	0	0	0	1	1	0
9. Décision relative au secret de l'instruction	0	0	0	0	0	0	0	0
10. Informations sensibles lors de l'audition	0	0	0	0	0	0	0	0
Décisions finales								
11. Cessation de la méthode	3	3	6	9	4	11	10	5
12. Cessation partielle de la méthode	10	13	4	6	6	4	0	3
13. Levée (partielle) de l'interdiction de la Commission BIM	0	4	11	0	0	0	0	0
14. Non compétent	0	0	0	0	0	0	0	0
15. Autorisation légale/ Non- cessation de la méthode/Non-fondement	4	6	2	1	1	0	0	1
Avis préjudiciels								
16. Avis préjudiciel	0	0	0	0	0	0	0	0

[233] Le Comité demande au service d'Enquêtes d'effectuer des recherches complémentaires et/ou de contacter le service concerné ou la Commission BIM.

II.2.2.2. La jurisprudence

La substance des décisions finales prises en 2021 par le Comité permanent R dans le cadre de son rôle juridictionnel en matière de contrôle des méthodes particulières de renseignement est reprise ci-après.[234] Les synthèses sont expurgées des données opérationnelles. Seuls sont mentionnés les éléments qui présentent un intérêt d'un point de vue juridique.

Les décisions ont été regroupées dans les rubriques suivantes :
- Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode ;
- La légalité d'une méthode quant aux techniques employées, aux données recueillies, à la durée de la mesure et à la nature de la menace ;
- La légalité de l'exécution d'une méthode légale.

Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode

SUBSIDIARITÉ, PROPORTIONALITÉ ET ORIENTATION DE LA MENACE

En vertu de l'article 18/3 § 1er, alinéa 1er L.R&S, une méthode spécifique ne peut être utilisée par un service de renseignement que s'il existe une menace potentielle pour les intérêts fondamentaux du pays qui relève de la compétence du service concerné. En outre, une telle MRD ne peut être mise en œuvre que si les méthodes ordinaires de collecte de données sont jugées insuffisantes pour recueillir les informations nécessaires à l'accomplissement de la mission de renseignement (exigence de subsidiarité). Enfin, la disposition légale susmentionnée impose le choix d'une méthode spécifique en fonction du degré de gravité de la menace potentielle pour laquelle elle est utilisée (exigence de proportionnalité).

Dans le dossier 2021/10548, un service de renseignement souhaitait obtenir les données de trafic et de localisation qui passaient par un numéro de téléphone spécifique.[235] La mise en œuvre de la méthode s'inscrivait dans le cadre d'une opération lancée par le service de renseignement pour savoir si un fonctionnaire donné était impliqué, sciemment ou non, dans des activités d'espionnage d'une puissance étrangère. En effet, le collaborateur avait été actif dans le pays concerné pendant de nombreuses années et certains comportements spécifiques ont amené le service de renseignement à se demander si un service de renseignement de cette puissance étrangère avait utilisé un « piège à miel » (*'honey trap')* ; autrement dit qu'un service étranger avait tenté, par des avances manipulatrices, amoureuses et sexuelles, d'obtenir des informations de la part de cette personne. Le profil de ce collaborateur, selon le service de renseignement concerné, correspondait au profil jugé intéressant par les services de renseignement étrangers pour l'utilisation

234 Dans certains dossiers, le Comité a été saisi en 2020, mais n'a rendu sa décision finale qu'en 2021.
235 *Cf.* article 18/8, § 1er, alinéa 1er, 1° et 2° L.R&S.

d'un tel procédé. En demandant les données relatives au trafic et à la localisation, un service de renseignement belge voulait identifier les contacts sociaux et professionnels du collaborateur concerné. Il a ensuite été possible de vérifier si ces contacts étaient légaux dans le cadre de l'exercice de son travail ou s'il s'agissait de contacts non officiels, irréguliers et/ou non autorisés, susceptibles de constituer une menace.

La Commission BIM a décidé de suspendre la mise en œuvre de cette méthode spécifique. Elle a estimé que les arguments et les éléments factuels avancés par le service de renseignement ne démontraient pas qu'il existait des raisons sérieuses et factuelles de supposer la présence d'indices à l'encontre de l'intéressé selon lesquels il aurait participé à des activités de renseignement clandestines pour un service de renseignement étranger. La Commission a établi que le comportement invoqué par le service de renseignement était insuffisant pour conclure que le collaborateur aurait pu faire l'objet d'un '*honey trap*'. La Commission BIM a également estimé que le service de renseignement n'avait pas suffisamment étayé le fait que les méthodes demandées étaient proportionnées à la gravité de la menace et que l'objectif poursuivi par les méthodes, compte tenu de l'état d'avancement de l'enquête de renseignement, ne pouvait être atteint de manière moins intrusive (subsidiarité). En ce qui concerne ce dernier aspect, la Commission était d'avis que de nombreuses informations pouvaient être obtenues par des méthodes ordinaires (par ex. une enquête de personnalité du *target*).

Conformément à l'article 43/4 L.R&S, le Comité permanent R est saisi de plein droit chaque fois que la Commission a suspendu l'utilisation d'une méthode spécifique ou d'une méthode exceptionnelle pour cause d'illégalité et a interdit l'exploitation des données pour cause d'illégalité d'une méthode spécifique ou d'une méthode exceptionnelle. Contrairement à la Commission, le Comité a considéré que le comportement invoqué par le service de renseignement était suffisant pour démontrer l'existence d'une menace potentielle, du moins en combinaison avec la position spécifique de la personne concernée, la position sensible qui y est associée et le profil (privé) spécifique de la personne concernée. Le Comité a également jugé que les exigences de subsidiarité et de proportionnalité avaient été respectées par le service de renseignement.

PROCÉDURE PARTICULIÈRE D'AUTORISATION POUR LES CATÉGORIES PROFESSIONNELLES PROTEGÉES

Dans son *Rapport d'activités 2020*, le Comité permanent R a indiqué qu'au cours de cette année de référence et pour la première fois depuis l'entrée en vigueur de la Loi MRD du 4 février 2010, il avait soumis une question préjudicielle à la Cour constitutionnelle concernant la législation MRD (dossier 2020/9606).[236]

[236] COMITÉ PERMANENT R, *Rapport d'activités 2020*, 94-97.

La question portait sur la décision d'un service de renseignement d'utiliser les méthodes spécifiques visées à l'article 18/8, § 1, 1° et 2° L.R&S sur un numéro de téléphone utilisé par un médecin. La mise en œuvre d'une méthode ordinaire a permis de constater que le numéro de téléphone en question n'était enregistré en Belgique qu'au nom de l'intéressé. Bien que le service de renseignement savait qu'il avait affaire à un médecin, il a suivi la procédure classique d'autorisation de méthodes spécifiques.[237] La Commission BIM n'était pas de cet avis et a suspendu les méthodes en cours. Compte tenu de la qualité de médecin de la personne visée, la Commission a estimé qu'il fallait recourir à la procédure d'autorisation spéciale pour les catégories professionnelles protégées prévue à l'article 18/3, § 5 L.R&S: *« (l)es méthodes spécifiques ne peuvent être mises en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la condition que le service de renseignement et de sécurité dispose au préalable d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur le projet de décision du dirigeant du service* ». Ce régime de protection particulière signifie que si un service de renseignement veut utiliser une méthode spécifique à l'égard de médecins, d'avocats ou de journalistes, il doit suivre la procédure d'autorisation des méthodes exceptionnelles. Ainsi, chaque méthode est soumise au contrôle préalable de la Commission BIM. En plus de la suspension de la méthode concernée, la Commission BIM a imposé une interdiction d'utiliser les données déjà obtenues.

L'ordonnance de suspension de la Commission BIM a donné lieu à une saisine d'office par le Comité permanent R. Compte tenu de l'importance du régime particulier de protection des catégories professionnelles susmentionnées, et en sa qualité d'organe juridictionnel[238] dans le cadre du contrôle des méthodes spécifiques et exceptionnelles, le Comité a décidé de soumettre à la Cour constitutionnelle la question préjudicielle suivante : *« L'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité viole-t-il les articles 10 et 11 de la Constitution, lus seuls ou conjointement avec l'article 22 de la Constitution et/ou combinés ou non avec l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 et approuvée par la loi du 13 mai 1955, en tant qu'il ne prévoit pas en faveur de l'avocat, du médecin ou du journaliste de protection particulière pour les moyens de communication qu'ils utilisent à des fins autre que professionnelles ?* ». En effet, le Comité a noté que l'article 18/2, § 3, alinéas 1er et 2 L.R&S limite la protection accordée aux avocats, médecins et journalistes aux moyens de communication qu'ils utilisent à des fins professionnelles. Il ressort du texte actuel de la disposition susmentionnée que

237 Immédiatement après que le service de renseignement s'est rendu compte de son erreur, une nouvelle demande, qui tenait compte du caractère protégé de la profession, a été introduite.

238 Cour constitutionnelle, 22 septembre 2011, n°145/2011, cons. B.38.1

les moyens de communication utilisés à des fins autres que professionnelles ne relèvent pas (ne semblent pas relever) de la protection juridique.

En avril 2021, la Cour constitutionnelle a statué en ces termes : « *Sous réserve de l'interprétation mentionnée en B.15.2, l'article 18/2, § 3, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ne viole pas les articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 8 de la Convention européenne des droits de l'homme.* »[239] Le considérant B.15.2 s'énonce comme suit : « *Eu égard à la protection particulière censée s'appliquer à toutes les informations médicales, notamment en vertu de la jurisprudence de la Cour européenne des droits de l'homme et du droit pénal belge, l'article 18/2, §3 de la loi du 30 novembre 1998 doit s'interpréter comme obligeant les services de renseignement et de sécurité à appliquer la protection offerte par le législateur en ce qui concerne les moyens de communication utilisés à des fins professionnelles lorsqu'il n'est pas certain que le moyen de communication qu'un médecin a utilisé l'a été exclusivement à des fins autres que professionnelles.* »

Suite à l'arrêt de la Cour constitutionnelle, le Comité permanent R a pris une décision finale dans le présent dossier MRD : « *Vu la qualité de médecin de [la personne X] et en rappelant l'arrêt n°64/2021 du 22 avril 2021 de la Cour Constitutionnelle, [le service de renseignement concerné] est obligé, dans le présent dossier, de démontrer que le moyen de communication en question utilisé l'est exclusivement à des fins autres que professionnelles, et ce afin que [le service de renseignement concerné] puisse utiliser en toute légalité la procédure ordinaire pour les méthodes spécifiques. Le Comité constate que la motivation de [le service de renseignement concerné] dans la décision contestée se limite à indiquer que « le sélecteur XXX et apparu comme étant le seul enregistré à son nom en Belgique ». Cette constatation ne suffit pas à démontrer que le moyen de communication en question est utilisé par [la personne X] exclusivement à des fins autres que professionnelles. Par conséquent, [le service de renseignement concerné] a utilisé de manière irrégulière la procédure ordinaire qui s'applique aux méthodes spécifiques.* »

NOTIFICATION TARDIVE À LA COMMISSION BIM

Un service de renseignement souhaitait prolonger une méthode spécifique, à savoir l'observation à l'aide de moyens techniques d'un lieu accessible au public (dossier 2021/10346). Conformément à l'article 18/3, § 4 L.R&S, une prolongation (ou

239 Cour constitutionnelle, 22 avril 2021, n°64/2021.

un renouvellement) [240] d'une méthode spécifique ne peut avoir lieu qu'après une nouvelle décision du dirigeant du service et après une notification à la Commission BIM. La période autorisée de mise en œuvre de la première méthode spécifique s'est terminée le 25 du mois à minuit. Or, la décision du dirigeant du service de prolonger l'observation, bien que prise le 25, n'a été notifiée à la Commission BIM que le 26 à 9h45. Suite à l'interdiction d'exploitation prononcée par la Commission BIM, le Comité a ordonné une interdiction d'exploitation et une destruction des données obtenues pendant la période non couverte.

ABSENCE D'AVIS CONFORME VERBAL DU PRÉSIDENT DE LA COMMISSION BIM

Conformément à l'article 18/10, § 4, alinéa 1er L.R&S, une méthode exceptionnelle peut être autorisée verbalement par le dirigeant d'un service de renseignement en cas d'extrême urgence, mais seulement après un avis conforme verbal du président de la Commission BIM. Dans le dossier 2021/10612, un service de renseignement a initié une interception (visée à l'art. 18/17, §§ 1er et 3 L.R&S), par erreur et dans un contexte d'extrême urgence, sans l'avis conforme du président de la Commission. Le service de renseignement concerné a constaté lui-même cette erreur, a immédiatement averti la Commission BIM et a placé en quarantaine les données obtenues illégalement. Comme le prévoit la loi, la Commission a interdit l'exploitation des données concernées et en a informé le Comité permanent R, qui a ordonné la destruction des données obtenues illégalement.

La légalité d'une méthode quant aux techniques employées, aux données recueillies, à la durée de la mesure et à la nature de la menace

OBJET ERRONÉ DE LA MÉTHODE

Dans le dossier 2020/10180, il s'est avéré que le service de renseignement avait par erreur inclus dans son autorisation un numéro de téléphone qui n'était pas couvert par la méthode spécifique concernée, à savoir la demande de données relatives au trafic et à la localisation des communications électroniques visée à l'article 18/8, § 1er, alinéa 1er, 1° et 2° L.R&S. Ce numéro d'appel erroné a également été mentionné dans la demande ultérieure adressée à l'opérateur de télécommunications. Mais le service s'en est lui-même aperçu, alors qu'il avait déjà reçu de l'opérateur de

[240] Bien que l'article 18/3, § 4 L.R&S ne fasse pas de distinction entre une « prolongation » d'une méthode spécifique et un « renouvellement » quant aux conditions formelles à respecter (c'est-à-dire la décision du dirigeant de service et la notification à la Commission BIM), un service de renseignement devrait être plus attentif à la gestion de la méthode concernée dans le cas d'une prolongation. Sinon, le risque existe que des périodes pendant lesquelles une méthode spécifique est en cours ne soient pas couvertes par une décision notifiée, ce qui entraîne alors une collecte illégale de données. Voir également : COMITÉ PERMANENT R, *Rapport d'activités 2020*, 97-98.

télécommunications les données réclamées. Le service de renseignement a lui-même pris l'initiative de placer les données obtenues en quarantaine électronique et a informé la Commission BIM de cette erreur. La Commission a interdit l'utilisation des données obtenues illégalement, a informé le Comité permanent R, qui a ordonné la destruction des données obtenues illégalement.

DURÉE DE LA MÉTHODE

En vertu de l'article 18/10, § 2 L.R&S, le projet d'autorisation concernant la mise en œuvre d'une méthode exceptionnelle doit, sous peine d'illégalité, indiquer la période pendant laquelle la méthode peut être utilisée. La procédure d'autorisation légale pour les méthodes exceptionnelles requiert ensuite un avis conforme de la Commission BIM. Avant de rendre cet avis, la Commission vérifie la légalité, la subsidiarité et la proportionnalité. L'un des aspects à vérifier par la Commission est la période de mise en œuvre proposée.

Dans le dossier 2021/10428, un service de renseignement avait demandé une prolongation pour une opération d'écoute téléphonique telle que visée à l'article 18/17, §§ 1er et 2 L.R&S.

Toutefois, le projet d'autorisation prévoyait deux périodes de mise en œuvre différentes (à savoir un mois *vs* deux mois). La Commission a rendu un avis conforme sur ce projet d'autorisation et a accepté une période de mise en œuvre de deux mois. Il est important de noter, cependant, que l'avis conforme de la Commission ne s'étendait pas sur la mention, dans le projet d'autorisation, de deux périodes de mise en œuvre différentes. Il n'est donc pas certain qu'un choix délibéré ait été opéré entre les deux périodes proposées par le service concerné. Le Comité permanent R s'est saisi d'office dans ce dossier. Il a établi *'dat de vermelding van deze verschillende data (1 maand, respectievelijk 2 maanden) in het ontwerp van machtiging waarschijnlijk op een materiële vergissing berust.'*[241] Le Comité a cependant estimé *'dat, zelfs bij een materiële vergissing, met het oog op het streven naar duidelijkheid en rechtszekerheid, een uitzonderlijke methode enkel kan worden toegestaan voor de kortste periode vermeld in het ontwerp van machtiging.'*[242] Le Comité a décidé que la méthode exceptionnelle était légale pour une période d'un mois à compter de l'autorisation du dirigeant du service.

---

241 *« que la mention de ces dates différentes (respectivement 1 mois et 2 mois) dans le projet d'autorisation est probablement due à une erreur matérielle »* (traduction libre).

242 *« que, même en cas d'erreur matérielle, dans un souci de clarté et de sécurité juridique, une méthode exceptionnelle ne peut être autorisée que pour la période la plus courte prévue dans le projet d'autorisation »* (traduction libre).

La légalité de l'exécution d'une méthode légale

DONNÉES RECUEILLIES PAR ERREUR

Dans trois dossiers distincts (2021/10533, 2021/10550 et 2021/10982), le service de renseignement concerné avait légalement décidé de rechercher des communications électroniques et de localiser l'origine ou la destination de communications électroniques.[243] Cependant, la transmission des données réclamées a posé un problème dans la mesure où les données transmises par le service NTSU-CTIF[244] ne correspondaient pas aux données réclamées. Dans le cas présent, en raison d'une erreur de manipulation de la part du service NTSU-CTIF, une écoute a systématiquement été lancée au lieu d'une localisation[245]. Il s'agissait donc d'un acte illégal, indépendant de la volonté du service de renseignement, ce que ce dernier a lui-même établi dans les trois cas. La Commission BIM et le NTSU-CTIF ont été immédiatement informés après chaque constatation. Dans les trois cas, le service de renseignement concerné a également décidé de son propre chef de rendre inaccessibles les données obtenues de manière irrégulière. La Commission BIM a émis à chaque fois une interdiction d'exploitation, qui a été suivie d'une ordonnance de destruction par le Comité permanent R.

II.3. CONSTATATIONS GÉNÉRALES

Le Comité permanent R formule les constatations générales suivantes :

- Entre le 1er janvier 2021 et le 31 décembre 2021, 1823 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 1570 par la VSSE (1220 spécifiques et 350 exceptionnelles) et 253 par le SGRS (166 spécifiques et 87 exceptionnelles). Après une augmentation constante du nombre total de MRD mises en œuvre ces dernières années et une stagnation observée en 2019-2020, on remarque une diminution considérable en 2021.
- La VSSE continue de se tailler la part du lion, avec 86 % des méthodes mises en œuvre. Un léger mouvement de rattrapage est constaté dans le chef du SGRS.
- Une ventilation de ces chiffres permet de constater une augmentation considérable du nombre de méthodes mises en œuvre par le SGRS (environ 30%), aussi bien pour les méthodes spécifiques (passant de 146 à 166) que

243 *Cf.* article 18/8, § 1er, alinéa 1er, 2° L.R&S (méthode spécifique).

244 Le service NTSU-CTIF (*National Technical & Tactical Support Unit – Central Technical Interception Facility*) est le système central d'interception technique de la police intégrée. Voir : Arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques.

245 Cf. article 18/17 L.R&S (méthode exceptionnelle).

les méthodes exceptionnelles (passant de 51 à 87). À la VSSE, on observe la tendance inverse, c'est-à-dire une diminution remarquable par rapport à 2020 de l'utilisation des méthodes spécifiques (de 1629 à 1220) ainsi que des méthodes exceptionnelles (de 511 à 350).

- En ce qui concerne les méthodes ordinaires de réquisitions adressées aux opérateurs afin d'identifier certains moyens de communication, on note de nouveau une diminution, que ce soit pour la VSSE ou le SGRS. Cependant, le nombre de 'sélecteurs' concernés par ces méthodes a augmenté au SGRS de près de 20 %, et est resté stable à la VSSE.
- Pour la première fois, les deux services de renseignement ont eu recours à la méthode ordinaire plus 'utilisation des images des caméras de police'. Le nombre de recherches ciblées au sein des données PNR a considérablement augmenté pour les deux services.
- Aucune conséquence n'a pu être constatée pour l'heure par les services de renseignement à l'annulation par la Cour constitutionnelle de la loi relative à la rétention des données.
- À la VSSE, on peut encore noter que les MRD mises en œuvre dans le cadre des menaces 'terrorisme' et 'espionnage' ont diminué en nombre, mais continuent d'occuper le haut du classement. Une hausse du nombre de dossiers 'ingérence' a été constatée ; la menace 'extrémisme-radicalisme' est restée stable en nombre de MRD.
- Au SGRS, une augmentation considérable a été constatée du nombre de MRD mises en œuvre dans le cadre de la menace 'extrémisme-radicalisme', due au dossier Jürgen Conings et l'attention spécifique accordée à la présence de l'extrême droite au sein de la Défense à la suite de celui-ci. La menace 'espionnage' est celle pour laquelle le plus de MRD ont été mises en œuvre.
- Le SGRS n'a pas (encore) mis en œuvre de MRD à l'étranger. Une enquête plus approfondie devrait permettre d'établir si c'est effectivement le cas ou s'il a été fait usage (à tort) des possibilités offertes par l'article 44 L.R&S. Une telle enquête s'inscrirait d'ailleurs dans la logique de la Loi du 30 mars 2017 dont l'exposé des motifs indiquait *« dans cinq ans, il sera procédé à une nouvelle évaluation de la situation pour voir si les prérogatives en faveur du SGRS sont praticables à l'étranger et si elles couvrent suffisamment les mandats des Nations Unies »*.
- Le Comité a été saisi dans 9 dossiers, à savoir 1 saisine d'initiative et 8 saisines de plein droit, après la suspension décidée par la Commission BIM pour illégalité (art. 43/4 L.R&S). Les illégalités concernaient notamment des problèmes quant à la durée ou l'objet des méthodes, la réception des données erronées ou encore, la notification tardive de la Commission BIM.
- En 2020, pour la première fois depuis l'entrée en vigueur de la Loi MRD, le Comité permanent R a posé une question préjudicielle à la Cour constitutionnelle concernant la législation MRD. En avril 2021, la Cour s'est prononcée sur celle-ci.

Le choix opéré par le législateur MRD en 2010 visant à établir une structure logique dans la Loi relative aux services de renseignement en ce qui concerne les compétences (d'enquête) des services de renseignement (entre autres une distinction entre les méthodes exceptionnelles, spécifiques et ordinaires en fonction du degré d'ingérence dans la vie privée) a été largement abandonné par les modifications législatives apportées ces dernières années. Les récentes propositions de modifications à la loi relative aux services de renseignement[246] n'améliorent guère la situation. Le Comité déplore que cette réglementation devienne ainsi trop complexe et incohérente. Une initiative législative, à laquelle le Comité est prêt à collaborer, s'avère nécessaire et offrira une sécurité juridique plus grande pour les services de renseignement mais aussi pour le citoyen.

246 Voir à ce propos 'VI.4. Avis concernant l'avant-projet de loi modifiant la loi organique des services de renseignement'.

CHAPITRE III.
LE CONTRÔLE DES INTERCEPTIONS À L'ÉTRANGER, DES PRISES D'IMAGES ET DES INTRUSIONS DANS DES SYSTÈMES INFORMATIQUES

III.1. LES COMPÉTENCES DU SGRS ET LA MISSION DE CONTRÔLE DU COMITÉ PERMANENT R[247]

Dès 2017, la compétence du Service Général du Renseignement et de la Sécurité (SGRS) a été élargie dans le cadre des interceptions de sécurité.[248] Les interceptions pouvaient alors porter sur des communications *'émises ou reçues à l'étranger'*. Cette possibilité vaut pour presque toutes les missions du SGRS. Il est d'ailleurs intéressant d'observer que les descriptions des missions ont, elles aussi, été élargies. Le législateur a en même temps introduit deux autres méthodes, à savoir 'l'intrusion dans un système informatique' (art. 44/1 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S)) et 'la prise d'images animées' (art. 44/2 L.R&S). Par ailleurs, la manière dont le Comité peut contrôler ces méthodes a été modifiée.

Le contrôle *préalable* aux interceptions, prises d'images fixes ou animées s'effectue sur la base d'une liste établie annuellement.[249] Cela signifie qu'en plus du plan annuel d'interceptions, le SGRS doit également élaborer un plan d'intrusions et d'images.[250] Le SGRS doit envoyer ces listes au ministre de la Défense au mois de décembre pour autorisation. Le ministre prend une décision endéans les dix

---

247 Voir articles 44 à 44/5 inclus L.R&S.

248 À propos des modifications de loi successives relatives à la compétence d'interception, voir COMITÉ PERMANENT R, *Rapport d'activités 2018*, 63 et suiv.

249 Ceci n'implique pas que le Comité permanent R a la compétence d'approuver ou non la liste approuvée par le ministre.

250 Dans ces plans, le SGRS dresse une liste *'d'organisations et d'institutions qui feront l'objet d'interceptions de leurs communications, d'intrusions dans leurs systèmes informatiques ou de prises d'images fixes ou animées dans le courant de l'année à venir. Ces listes justifieront pour chaque organisation ou institution la raison pour laquelle elle fera l'objet d'une interception, intrusion ou prise d'images fixes ou animées en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°, et mentionneront la durée prévue'* (art. 44/3 L.R&S).

jours ouvrables et doit la communiquer au SGRS[251], qui transmet à son tour les listes pourvues de l'autorisation ministérielle au Comité permanent R.[252]

Le contrôle réalisé *pendant* l'interception, l'intrusion ou la prise d'images s'effectue *'à tout moment moyennant des visites aux installations dans lesquelles le Service Général du Renseignement et de la Sécurité effectue ces interceptions, intrusions et prises d'images fixes ou animées'*.

Le contrôle réalisé *après* l'exécution s'effectue '*sur base de listes mensuelles des pays ou des organisations ou institutions ayant effectivement fait l'objet d'une écoute, d'une intrusion ou d'une prise d'images durant le mois écoulé*' et qui justifient '*la raison pour laquelle l'écoute, l'intrusion ou la prise d'images a été effectuée en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°*'. Ces listes doivent être notifiées au Comité permanent R. Le contrôle *ex post* s'effectue aussi sur la base *'du contrôle de journaux de bord tenus d'une façon permanente sur le lieu d'interception, d'intrusion ou de prise d'images fixes ou animées par le Service Général du Renseignement et de la Sécurité'*. Le Comité permanent R doit toujours avoir accès à ces journaux de bord.

Que peut faire le Comité permanent R en cas d'irrégularité ? L'article 44/4 L.R&S stipule que, '*le Comité permanent de contrôle des services de renseignement, sans préjudice des autres compétences attribuées à ce Comité par la loi du 18 juillet 1991, a le droit de faire cesser des interceptions, intrusions ou prises d'images en cours lorsqu'il apparaît que celles-ci ne respectent pas les dispositions légales ou l'autorisation [ministérielle]. Il ordonne l'interdiction d'exploiter les données recueillies illégalement et leur destruction, selon les modalités à fixer par le Roi.*' Malgré la recommandation pressante du Comité[253], un tel arrêté d'interception n'a toujours pas été pris.[254] Aussi, le Comité recommande une nouvelle fois de le faire au plus vite.

---

251 Si le ministre n'a pas pris de décision ou ne l'a pas transmise au SGRS avant le 1er janvier, le service peut procéder aux interceptions, intrusions et prises d'images fixes ou animées prévues, sans préjudice de toute décision ultérieure du ministre.

252 Pour les interceptions, les intrusions ou les prises d'images qui ne figurent pas dans les listes annuelles mais qui *'s'avèrent indispensables et urgentes'*, le ministre est averti dans les plus brefs délais, au plus tard le premier jour ouvrable qui suit le début de l'interception. S'il n'est pas d'accord, il peut faire cesser l'interception. Cette décision est communiquée au Comité permanent R le plus rapidement possible par le SGRS.

253 COMITÉ PERMANENT R, *Rapport d'activités 2018*, 131.

254 Le Comité doit de toute manière motiver sa décision de manière circonstanciée et la communiquer au ministre et au SGRS.

III.2. LES CONTRÔLES EFFECTUÉS EN 2021

III.2.1. LE CONTRÔLE PRÉALABLE À L'INTERCEPTION, L'INTRUSION OU LA PRISE D'IMAGES

L'ensemble des plans relatifs aux interceptions, aux intrusions et aux prises d'images pour l'année 2021 a été remis au Comité permanent R à la mi-janvier 2021.

Préalablement à la remise de ces documents, le SGRS a organisé une réunion de travail à leur sujet avec le Comité. Lors de celle-ci, le Comité a formulé un certain nombre de remarques quant aux prescrits légaux à respecter. À la réception des plans, le Comité permanent R a constaté que, conformément à ses recommandations, les trois plans (les plans relatifs aux interceptions, aux intrusions et aux prises d'images) avaient été regroupés dans un document unique. Le SGRS a ainsi visé à uniformiser à brève échéance l'ensemble des plans qu'il produit conformément à l'art. 44 L.R&S. Les autres remarques formulées ayant également été prises en compte, le Comité a pu conclure que les plans pour l'année 2021 respectent les prescrits légaux.

III.2.2. LE CONTRÔLE PENDANT L'INTERCEPTION, L'INTRUSION OU LA PRISE D'IMAGES

Le Comité permanent R a visité en 2021 les installations à partir desquelles sont effectuées les interceptions. Il a notamment pu vérifier, lors de sa visite, la conformité du *logbook* avec les lois et les directives d'application. Le Comité a relevé des manquements mineurs qui ont été immédiatement rectifiés par le responsable présent sur place.

Le Comité permanent R a également réalisé, pour la première fois, une inspection sur site du service du SGRS en charge de l'exécution du plan d'intrusion. À cette occasion, il a pu constater que le service atteignait progressivement son entière capacité opérationnelle. Il a rappelé les prescrits légaux d'application (et plus précisément l'obligation de tenir un *logbook*), et a invité le service à s'y conformer. Cet élément retiendra l'attention du Comité lors de ses visites ultérieures.

Quant au plan de prises d'images, le Comité permanent R n'a pas pu effectuer de contrôle des installations en 2021. Ce contrôle sera prioritairement réalisé en 2022.

III.2.3. LE CONTRÔLE APRÈS L'EXÉCUTION DE LA MÉTHODE

Le Comité a reçu douze '*listes mensuelles des pays ou des organisations ou institutions ayant effectivement fait l'objet d'une écoute, d'une intrusion ou d'une prise d'images durant le mois écoulé*' et qui justifient '*la raison pour laquelle l'écoute, l'intrusion ou la prise d'images a été effectuée en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°*'.

Le Comité permanent R a donc reçu l'ensemble des listes légalement prévues. Il évaluera la forme et le contrôle lié auxdites listes avec le SGRS courant 2022.

CHAPITRE IV.
LE COMITÉ PERMANENT R EN SA QUALITÉ D'AUTORITÉ DE CONTRÔLE COMPÉTENTE DANS LE CADRE DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

IV.1. INTRODUCTION

Le Règlement Général sur la Protection des Données 2016/679 (RGPD)[255] et la Directive 2016/680 (Directive)[256] règlent la manière dont les acteurs publics et privés doivent opérer lorsqu'ils collectent, sauvegardent, conservent et communiquent des données à caractère personnel. Les deux instruments européens ont donné lieu à quelques modifications de loi substantielles au niveau national : en décembre 2017, l'Autorité de protection des données (APD) [257] – qui a succédé à la Commission Vie privée – a été créée et en juillet 2018, une nouvelle Loi relative à la protection des données (LPD) a été votée.[258] Cette loi modifie à son tour la L.Contrôle du 18 juillet 1991. Le Comité permanent R a, en effet, été désigné comme autorité de contrôle compétente pour les traitements de données à caractère personnel qui relèvent de la 'sécurité nationale'.

Le rôle du Comité en la matière est décrit dans la Loi portant création de l'Autorité de protection des données (Loi APD), dans la Loi relative à la protection des données (LPD) et dans la Loi organique du contrôle des services de police

---

255 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD), Journal Officiel de l'Union européenne, 2 mai 2016.

256 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes, de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la Décision-cadre 2008/977/JAI du Conseil, Journal Officiel de l'Union européenne, 4 mai 2016, n° 119/89.

257 Loi du 3 décembre 2017 portant création de l'Autorité de protection des données (Loi APD), *M.B.* 10 janvier 2018.

258 Dénomination complète : Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD), *M.B.* 5 septembre 2018.

et de renseignement et de l'Organe de contrôle pour l'analyse de la menace (L.Contrôle).[259]

L'article 35 § 3 L.Contrôle énonce que le '*Comité permanent R fait rapport annuellement à la Chambre des représentants sur les avis rendus en sa qualité d'autorité de protection des données, sur les enquêtes effectuées et mesures prises en cette même qualité ainsi que sur sa collaboration avec les autres autorités de protection des données*'. Ce chapitre répond à cette obligation. Il aborde successivement les thèmes suivants :

- les contrôles effectués par le Comité – seul ou avec l'Organe de contrôle de l'information policière (C.O.C.) ou le Comité P – à la demande de citoyens qui souhaitent exercer leur droit d'accès indirect à leur 'dossier' dans l'un des services contrôlés par le Comité ;
- les avis rendus par le Comité concernant la protection des données ;
- la notification d'une potentielle brèche de sécurité ;
- les travaux dans le cadre de l'évaluation de loi sur la protection des données.

IV.2. LE TRAITEMENT DES REQUÊTES INDIVIDUELLES

Le Comité permanent R est compétent pour le traitement des requêtes individuelles relatives aux traitements de données à caractère personnel par les personnes et les services susmentionnés ainsi que leurs sous-traitants (art. 34 L.Contrôle et articles 79, 113, 145 et 173 LPD). Le requérant est en droit de demander la rectification ou la suppression de données à caractère personnel inexactes le concernant. Et il peut demander à ce que le respect des règles qui sont d'application en matière de protection des données soit vérifié. Il peut encore se plaindre de l'éventuel non-respect des règles de protection des données par un responsable du traitement relevant de la compétence du Comité.

Pour être recevable, une requête doit être écrite, datée, signée et motivée (art. 51/2 L.Contrôle).[260] Si la requête est manifestement non fondée, le Comité peut décider de ne pas y donner suite. Cette décision doit être motivée et communiquée par écrit au requérant.[261]

Le tableau suivant donne un aperçu des dossiers traités (ouverts et/ou clôturés) en 2021. Les colonnes du tableau ventilent les requêtes selon que la compétence du

---

259 Pour plus de détails, voir COMITÉ PERMANENT R, *Rapport d'activités 2018*, 75-86.

260 Cette disposition stipule également que la requête doit '*justifier de l'identité de la personne concernée*'. Il est difficile de saisir d'emblée la signification de cette disposition. Il s'agit vraisemblablement de l'obligation de prouver son identité. Cette obligation est en fait reprise dans les dispositions concernées de la Loi relative à la protection des données (voir les articles 80, 114, 146 et 174 LPD).

261 Ces vérifications sont effectuées sans frais (voir les articles 80, 114, 146 et 174 LPD).

Comité permanent R est exclusive ou conjointe avec d'autres autorités de contrôle (AC).[262]

Tableau 1. Le traitement des requêtes individuelles[263]

2021	Comité permanent R		Comités permanents R et P	Comités permanents R et P et le C.O.C.	**Total**
1. Dossiers ouverts en 2021	14		2	0	**16**
2. Requêtes irrecevables en 2021	3		0	0	**3**
3. Requêtes recevables en 2021	8		0	0	**8**
	c. SGRS	2			
	c. VSSE	6			
	c. VSSE&SGRS	-			
4. Requêtes en suspens en 2021	3		0	0	**0**
5. Dossiers en cours en 2021	10[264]		1	2[265]	**13**
6. Dossiers clôturés en 2021[266]	10[267]		2[268]	1[269]	**13**
7. Mesures correctives	3		0	1	**4**
8. Nombre total de requêtes traitées	20		3	3	**26**

262 Le tableau n'indique donc pas les hypothèses dans lesquelles une coopération a pu se réaliser avec une autre autorité de contrôle, le C.O.C. par exemple, lorsque les compétences de chaque AC sont distinctes.

263 La ligne 1 indique le nombre de dossiers ouverts en 2021. Les lignes 2 et 3 répartissent les requêtes selon la décision d'irrecevabilité ou de recevabilité. Pour les dossiers traités uniquement par le Comité permanent R, la ligne 3 précise encore le nombre de requêtes recevables selon les services visés. À la ligne 4 figure le nombre de requêtes dont la décision de recevabilité est encore en suspens. Les lignes 5 et 6 précisent l'état d'avancement des dossiers en 2021 (toujours en cours ou clôturés). Enfin, la ligne 7 indique le nombre de dossiers pour lesquels des mesures correctives ont été exigées par le Comité.

264 Dont un dossier ouvert en 2020.

265 Dont deux dossiers ouverts en 2020.

266 Complètement clôturés. Lorsque des mesures correctives sont exigées, le Comité permanent R clôture le dossier lorsqu'il a pu constater que les mesures ont été mises en œuvre.

267 Dont cinq dossiers ouverts en 2020.

268 Dont un dossier ouvert en 2020.

269 Dont un dossier ouvert en 2020.

Il peut être relevé que dans 85 % des requêtes, les personnes concernées allèguent[270] une interférence concrète dans leurs droits et libertés causée par, ou en tout cas liée à, un traitement de données d'un responsable du traitement relevant de la compétence du Comité permanent R. Une telle interférence existerait, par exemple, dans le cadre d'une demande d'acquisition de la nationalité ou de titre de séjour à l'occasion de laquelle un service de renseignement communique des informations au Ministère public, lorsque la personne concernée allègue faire l'objet de contrôles réguliers de police, lorsqu'elle constate que l'accès à un territoire lui est refusé, lorsque des données d'un service de renseignement ont été utilisées dans une procédure judiciaire pénale.

En 2021, le Comité a ainsi eu à traiter plusieurs requêtes déposées dans le cadre de procédures de demande de nationalité ou de droit de séjour. Confrontés à une décision négative motivée sur la base d'informations fournies par la Sûreté de l'État (VSSE), le Service Général du Renseignement et de la Sécurité (SGRS) et/ou l'Organe de coordination pour l'analyse de la menace (OCAM), les requérants s'adressent (entre autres) au Comité permanent R pour un contrôle du traitement de leurs données personnelles.

Une requête déposée en 2020 a également donné lieu à l'ouverture en 2021 d'un dossier d'information. Lors du traitement de la requête, le Comité permanent R a en effet constaté des pratiques non conformes au prescrit légal. À partir d'une requête individuelle, le Comité a ainsi souhaité interroger le traitement général des données à caractère personnel par les services de renseignement dans un contexte spécifique.

Les 15 % restant de requêtes se composent de demandes d'exercice indirect de droits, sans précision particulière ou grief concret. Typiquement, la personne concernée se demande si des données sont traitées à son sujet et si le traitement de celles-ci est conforme à la réglementation applicable (accès indirect).

Ce déséquilibre (85-15 %) n'est pas surprenant dès lors que la réponse fournie à la personne concernée exerçant ses droits ne lui apprend rien sur ce qu'il en est du traitement (éventuel) de ses données à caractère personnel par les services relevant de la compétence du Comité. Ce n'est que lorsque la personne concernée suspecte ou subit concrètement l'effet d'un tel traitement de données, qu'elle verra un intérêt à s'adresser au Comité permanent R pour qu'il réalise les vérifications nécessaires, dans l'espoir d'obtenir une amélioration de sa situation.

---

[270] Il est à noter que dans plusieurs dossiers, ces interférences ne sont pas seulement alléguées par les personnes concernées mais bien étayées par elles et avérées (s'agissant par exemple, de la communication de notes d'analyse dont disposent les personnes concernées dans le cadre des procédures où ces notes sont utilisées par les autorités publiques). Dans d'autres cas, ces allégations sont des suspicions, plus ou moins, voire non, étayées en fait.

IV.3. LES AVIS

Le Comité peut rendre un avis *'sur un projet de loi, d'arrêté royal, de circulaire, ou sur des documents de toutes natures exprimant des orientations politiques des ministres compétents'* dans deux cas : lorsque la loi impose son avis ou à la demande de la Chambre des représentants ou du ministre compétent (art. 33, alinéa 8 L. Contrôle). Ce genre d'avis porte spécifiquement sur la problématique du traitement de données et doit donc être distingué de la compétence d'avis générale qui porte, par exemple, sur l'efficacité et la coordination (cf. Chapitre VI. Avis). Cette compétence d'avis générale est, en ce sens, plus large, tout en étant plus restreinte puisque limitée au fonctionnement des services de renseignement et de l'OCAM.

En 2021, le Comité a rendu trois avis en cette qualité, dont deux portent sur l'échange d'informations classifiées[271] et un sur l'avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace en tant qu'autorité conjointement compétente avec le Comité permanent P[272] :

- Avis 005/CPR/2021 du 1er décembre 2021 portant sur une demande d'avis du président de l'Autorité nationale de sécurité concernant le *'projet de loi portant assentiment à l'accord entre le Royaume de Belgique et le Royaume des Pays-Bas concernant l'échange et la protection mutuelle des informations classifiées, fait à Bruxelles le 5 novembre 2019'*.
- Avis 006/CPR/2021 du 1er décembre 2021 portant sur une demande d'avis du président de l'Autorité nationale de sécurité concernant le *'projet de loi portant assentiment à l'accord entre le Royaume de Belgique et le Royaume-Uni de Grande Bretagne et d'Irlande du Nord concernant la protection mutuelle des informations classifiées, fait à Bruxelles le 1 décembre 2020'*.
- Avis commun 001/CPR-CPP/2021 du 8 octobre 2021 sur '*l'avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace*'.

IV.4. LA NOTIFICATION D'UNE POTENTIELLE BRÈCHE DE SÉCURITÉ

Les services contrôlés par le Comité permanent R doivent conserver ou mettre à la disposition du Comité toute une série de données.[273] Le responsable du traitement

---

271 Des avis en ce sens avaient déjà été rendus en 2019 et 2020 sur l'échange d'informations classifiées avec la République de Chypre, la Hongrie, la République de Finlande et le Royaume d'Espagne, la République française et la République italienne.

272 Voir *in extenso* sur le site du Comité permanent R.

273 Chaque service n'est pas tenu de conserver ou tenir à disposition du Comité toutes les données mentionnées ici. La Commission BIM ne doit ainsi pas communiquer d'informations au Comité.

doit ainsi notifier toute brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques dans les meilleurs délais et si possible, 72 heures après en avoir pris connaissance (articles 89, 122, 155 et 180 LPD).

En 2021, la presse a fait état d'un piratage du réseau informatique du SPF Intérieur.[274] En réponse, le directeur de l'Unité belge d'information des passagers (BELPIU) a spontanément déclaré que le système informatique distinct des dossiers passagers (PNR) n'avait pas été compromis. C'est ce qu'a révélé une analyse effectuée par le Centre pour la Cybersécurité Belgique (CCB).

IV.5. ÉVALUATION DE LA LOI RELATIVE À LA PROTECTION DES DONNÉES

L'article 286 LPD dispose que la Loi relative à la protection des données doit être soumise à une évaluation conjointe des ministres compétents dans le courant de la troisième année après son entrée en vigueur. Dans ce contexte, le secrétaire d'État Mathieu Michel a écrit au Comité permanent R pour lui demander son aide dans le cadre du comité d'orientation qu'il a mis en place. Le Comité a ensuite fourni plusieurs documents contenant des propositions aussi bien générales que technico-juridiques très spécifiques pour renforcer la protection des données.[275]

[274] H. DECREM et L. BELGHMIDI, www.vrt.be, 26 mei 2021 ('Twee jaar lang 'doelbewuste cyberaanval op overheidsdienst Binnenlandse Zaken: 'Dit is spionage").

[275] Voir à cet égard : COMITÉ PERMANENT R, *Rapport d'activités 2020*, 119-125, ('V.7. Évaluation de la loi relative à la protection des données').

CHAPITRE V.
LE CONTRÔLE DES BANQUES DE DONNÉES COMMUNES

La création de la banque de données commune '*foreign terrorist fighters*' par les ministres de l'Intérieur et de la Justice remonte à 2016. Cette banque de données commune a été modifiée en 2018 : on parle désormais de la banque de données commune '*terrorist fighters*' (BDC TF). Celle-ci comprend, outre la catégorie générale des '*foreign terrorist fighters*', une catégorie visant les '*homegrown terrorist fighters*'. Toujours en 2018, une (nouvelle) banque de données commune distincte a été créée pour les 'propagandistes de haine' (BDC PH). Par un arrêté royal pris fin 2019, deux nouvelles catégories ont encore été ajoutées à la BDC TF, à savoir les 'extrémistes potentiellement violents' (EPV) ainsi que les 'personnes condamnées pour terrorisme' (PCT).

L'article 44/11/3*quinquies*/2 LFP assigne le contrôle du traitement des informations et des données à caractère personnel contenues dans les banques de données communes à l'Organe de contrôle de l'information policière (C.O.C.) et au Comité permanent R (ci-après "les autorités de contrôle"). Un rapport conjoint a été établi dans le cadre de ce contrôle. Il fut discuté début octobre 2021 au sein de la Commission de suivi.[276]

V.1. LA MISSION DE CONTRÔLE ET L'OBJET DU CONTRÔLE

Pour l'année 2020-2021, le Comité permanent R et le C.O.C. ont décidé d'axer leur contrôle conjoint, d'une part, sur la vérification de l'accès direct prévu en faveur de l'Autorité nationale de sécurité (ANS) et, d'autre part, sur le suivi réservé à certaines recommandations formulées dans les rapports des années précédentes.

Par ailleurs, les autorités de contrôle ont procédé à un examen approfondi de la coordination du traitement des informations dans la BDC TF et la BDC PH, avec notamment une attention particulière pour le rôle du *data protection officer* (DPO).

---

[276] C.O.C. et COMITÉ PERMANENT R, *Rapport concernant le contrôle conjoint des Banques de données communes Terrorist Fighters et Prédicateurs de haine par le Comité permanent R et l'Organe de contrôle de l'information policière*, 2020, 33 p. (Diffusion restreinte - A.R. 20 mars 2000). Le rapport a été approuvé par les autorités de contrôle le 12 août 2021.

À cet égard, le nombre croissant de services disposant d'un accès à la BDC TF et la BDC PH a également été pris en compte.

Sur le plan méthodologique, compte tenu de la crise sanitaire et afin de permettre aux services de disposer d'un recul suffisant pour la mise en œuvre des recommandations formulées au terme du rapport relatif au contrôle pratiqué en 2019, il a été décidé de prévoir le déroulement de l'enquête durant le quatrième trimestre de l'année 2020. Plusieurs services ont été questionnés, parmi lesquels l'ANS, l'OCAM (responsable opérationnel des banques de données communes), la Police fédérale (gestionnaire technique) ainsi que les *data protection officers* (DPO). L'enquête s'est clôturée par une rencontre avec le Directeur f.f. de l'OCAM ainsi que le DPO des banques de données communes.

V.2. LES CONSTATATIONS DE L'ENQUÊTE

V.2.1. L'ABSENCE D'ACCÈS DE L'ANS

Au moment du contrôle, le C.O.C. et le Comité permanent R ont constaté que l'ANS n'était pas reliée aux banques de données communes (BDC) et qu'elle n'avait entrepris aucune démarche en ce sens.

Le C.O.C. et le Comité permanent R ont estimé que l'ANS faisait preuve d'une nonchalance manifeste et irresponsable. Son abstention, qui contrevient à la réglementation en vigueur, a fait courir des risques de sécurité non seulement en ce qui concerne le caractère systématique de la consultation des BDC, mais aussi en ce qui concerne l'alimentation de celle-ci. La Police fédérale a indiqué qu'elle ne procédait pas à l'alimentation des BDC dans le cadre des vérifications de sécurité (ni des habilitations de sécurité). Rien n'indiquait que cette alimentation était systématiquement effectuée par les services de renseignement en ce qui concerne les habilitations de sécurité. De ce fait, différentes informations intéressantes, voire cruciales, ont potentiellement pu échapper aux services.

D'autre part, compte tenu du fait que l'ANS ne dispose pas d'une compétence exclusive en qualité d'autorité de sécurité, et afin d'assurer la complétude des BDC, le C.O.C. et le Comité permanent R recommandaient aux différentes autorités de sécurité visées aux articles 15, al.2 et 22*ter*, al.2 L.C&HS et 9, al.1, 9° de la Loi du 28 février 2007[277] de s'assurer de la consultation effective des BDC dans les différents processus pour lesquels elles sont compétentes et d'alimenter les BDC concernant leurs décisions, soit sur base de leur accès direct aux BDC soit en prenant contact avec un service de base à cette fin (dans le cas où elles ne disposent pas de l'accès direct).

[277] Loi du 28 février fixant le statut des militaires et candidats militaires du cadre actif des Forces armées, inséré par la Loi du 31 juillet 2013 modifiant ladite Loi, *M.B.* 20 septembre 2013.

Le C.O.C. et le Comité permanent R ont indiqué que ces différents aspects seront vérifiés lors des contrôles ultérieurs.

V.2.2. LE SUIVI DES RECOMMANDATIONS ANTÉRIEURES

V.2.2.1. Les recommandations suivies d'effet

La disponibilité et l'indépendance du DPO

Le contrôle a démontré que le DPO des BDC disposait des connaissances juridiques requises pour assurer la fonction. Le travail effectué est satisfaisant, ceci d'autant plus que les circonstances (crise sanitaire) n'ont pas facilité l'accomplissement de toutes les missions. Les problématiques de la charge de travail et de la disponibilité du DPO avaient été précédemment identifiées.[278] Dans le cadre du contrôle, il est apparu que le DPO avait depuis demandé un '*réajustement du temps de travail*'. Cette demande a été analysée par le service RH de l'OCAM. Le C.O.C. et le Comité permanent R ont insisté sur le fait que le DPO doit disposer de toute la liberté requise car, en raison du nombre élevé d'utilisateurs et de la technicité de la matière, sa mission est délicate et complexe. La détermination ou la validation des priorités (contenues dans une lettre de mission) par les responsables de traitement était également un facteur critique de succès. En ce qui concerne le risque de conflit d'intérêts, le contrôle effectué a permis de l'écarter : différents avis transmis par le DPO des BDC ont démontré qu'il dispose de l'indépendance requise.

V.2.2.2. Les recommandations non suivies d'effet

Le signalement des incidents de sécurité

Le C.O.C. et le Comité permanent R ont réitéré, à l'attention de la Police fédérale, leur recommandation de leur signaler formellement les incidents de sécurité. Le contrôle pratiqué a révélé un incident de sécurité n'ayant pas fait l'objet d'un signalement immédiat. Ce signalement relève de la responsabilité de la Police fédérale, en sa qualité de gestionnaire technique des BDC. Les autorités de contrôle ont, en outre, attiré l'attention de la Police fédérale sur le fait que la notion '*d'incident de sécurité*' vise non seulement la confidentialité, mais également la disponibilité et l'intégrité des BDC.

En ce qui concerne le suivi de la seconde recommandation (information adéquate des services utilisateurs quant au rapportage d'incidents constatés), le

[278] Voir à ce propos COMITÉ PERMANENT R, *Rapport d'activités 2019*, ('XI.2.4. Évaluation des conflits d'intérêts et de l'emploi du temps du délégué à la protection des données'), 133.

C.O.C. et le Comité permanent R ont posé le constat qu'il n'y avait pas eu d'avancée significative en 2020. Cette recommandation a également été réitérée.

V.2.2.3. Les recommandations partiellement suivies d'effet

L'exécution de développements informatiques

Le C.O.C. et le Comité permanent R ont constaté que leur recommandation relative à l'exécution de développements informatiques (en vue d'assurer le suivi des délais de conservation des données dans les BDC) semblait être en cours d'exécution. Un suivi était annoncé par la Police fédérale au début du second semestre 2021. Ils ont insisté pour que cet aspect, régulièrement rappelé depuis le début des contrôles conjoints, soit définitivement réglé dans le délai annoncé par la Police.

Le contrôle des loggings

D'autre part, le C.O.C. et le Comité permanent R ont constaté que leur recommandation en matière de contrôle de loggings était en cours d'exécution. La Police fédérale avait pris une initiative visant à encourager le contrôle des loggings par les services de police. Le C.O.C. et le Comité permanent R souhaitaient que le DPO des BDC, dans sa mission de stimulation de la sécurité de l'information, veille à ce que cette initiative soit étendue à tous les (DPO des) utilisateurs, ceci d'autant plus que certains d'entre eux n'ont pas l'habitude de traiter des informations sensibles. Lors du contrôle, il a été mentionné que la fonctionnalité de contrôle des loggings était prévue dans la version '3.0' des BDC. Le C.O.C. et le Comité permanent R ont insisté sur le fait que tous les services soient en mesure, lors d'un prochain contrôle, de démontrer qu'ils ont exécuté un contrôle des loggings.

L'exception à l'obligation d'alimenter les BDC et les informations policières

Les contrôles antérieurs ont révélé que les informations policières issues de « RIR, code 01 ou code 00 » n'étaient pas reprises dans les BDC.[279] Les autorités de contrôle avaient demandé à la Police fédérale d'analyser la réglementation relative à l'alimentation des BDC de manière approfondie. Le C.O.C. et le Comité permanent R estimaient que l'analyse de la Police fédérale n'était que partiellement satisfaisante. Une analyse plus approfondie et réalisée en concertation avec les autorités judiciaires a été demandée.

[279] Un « RIR 01 » concerne des informations policières qui ne peuvent être utilisées qu'avec l'accord du rédacteur. Un « RIR 00 » concerne des informations policières qui ne peuvent en aucun cas être utilisées.

La transmission des listes

Le C.O.C. et le Comité permanent R ont noté que des initiatives avaient été prises, d'une part, en vue de mettre fin (partiellement) à la transmission de listes qui ne répondait pas à la réglementation et, d'autre part, en vue de définir les principes clairs et d'élaborer des protocoles d'accord portant sur les finalités, les modalités et les aspects de sécurité de cette transmission. Ils ont salué les initiatives particulières prises par le DPO des BDC. Compte tenu de la réglementation (et sous réserve d'une modification de celle-ci suite à l'enquête menée par l'OCAM), la signature de protocoles s'impose pour tous les services qui ne disposent pas d'un accès direct aux BDC, avec une priorité à accorder aux services qui ne disposent d'aucun accès. Le C.O.C. et le Comité permanent R ont recommandé une analyse et une mise en œuvre rapide des propositions de protocoles d'accord du DPO.

La consultation du Ministère public par l'OCAM concernant les mesures judiciaires

La réglementation tient compte du statut indépendant du Ministère public puisqu'il n'y a aucune obligation (mais une possibilité) pour ce service partenaire d'alimenter la BDC TF et la BDC PH et ce, même s'il a un accès direct. Le législateur a jugé que les données judiciaires proviennent principalement de la police. En ce sens, l'obligation pour les services de police d'alimenter la banque de données commune suffit, de sorte que les données pertinentes de la Police judiciaire sont enregistrées.[280] Afin de s'assurer que les banques de données TF et PH soient correctement alimentées, les autorités judiciaires ont envoyé des instructions. Il n'est pas apparu pas que l'OCAM mettait en œuvre les principes énoncés par la COL 18/2020. Le C.O.C. et le Comité permanent R ont dès lors recommandé à l'OCAM la mise en œuvre des principes contenus dans cette COL, de manière à aboutir à une alimentation et à une mise à jour systématique des BDC.

En outre, sans préjudice du principe de séparation des pouvoirs et de l'autonomie des autorités judiciaires, le C.O.C. et le Comité permanent R ont invité le ministre de la Justice à faire adapter par le Collège des Procureurs généraux la circulaire COL 18/2020 quant à la communication des mesures judiciaires portant sur les extrémistes potentiellement violents (EPV).

V.2.3. DE NOUVELLES RECOMMANDATIONS

Suite à un incident de sécurité – le Service des Cultes et de la Laïcité du SPF Justice disposait d'un accès plus large à la BDC PH que ce que prescrit l'AR PH

[280] Le C.O.C. et le Comité permanent R ont cependant noté que ce raisonnement ne s'applique pas aux jugements et aux arrêts dont les services de police n'ont pas connaissance.

– le C.O.C. et le Comité permanent R ont interpellé les responsables de traitement. Ces derniers ont été invités à mettre un terme aux accès irréguliers. Les autorités de contrôle ont recommandé à la Police fédérale d'apporter les solutions techniques nécessaires pour mettre l'accès de ce service en conformité avec la législation en vigueur (soit accès indirect à la BDC PH uniquement). Le C.O.C. et le Comité permanent R souhaitaient être tenus impérativement et précisément informés à ce propos.

Par ailleurs, ils ont recommandé aux responsables de traitement d'évaluer, sur les plans juridique et opérationnel, si la règlementation de l'accès du Service des Cultes et de la Laïcité devait (ou non) être révisée.

V.3. LA MISSION D'AVIS

La Loi sur la fonction de police (LFP) prévoit également l'obligation de recueillir l'avis conjoint du Comité permanent R et du C.O.C. dans différentes hypothèses.

Ainsi, préalablement à sa création, les ministres de l'Intérieur et de la Justice doivent déclarer la banque de données commune ainsi que les modalités de traitement, dont celles relatives à l'enregistrement des données, et les différentes catégories et types de données à caractère personnel et d'informations traitées, au Comité permanent R et au C.O.C. À leur tour, le Comité et le C.O.C. doivent émettre conjointement un avis (art.44/11/3*bis* § 3 LFP). Par ailleurs, pour chaque banque de données commune, un Arrêté royal délibéré en Conseil des ministres détermine, après avis des deux instances précitées, les règles de responsabilités en matière de protection des données à caractère personnel des organes, services, autorités et organismes traitant des données, les règles en matière de sécurité des traitements, les règles d'utilisation, de conservation et d'effacement des données (art.44/11/3*bis* § 4 LFP). En outre, des modalités complémentaires de gestion des banques de données communes peuvent être déterminées par un arrêté royal délibéré en Conseil des ministres, toujours après un avis du Comité permanent R et du C.O.C. (art.44/11/3*bis* § 8 LFP). Enfin, la fonction d'avis s'exerce également en ce qui concerne tout projet d'Arrêté royal instaurant ou modifiant les accès aux banques de données communes (art.44/11/3*ter* §§ 2 à 4).

Le Comité permanent R et le C.O.C. n'ont pas été sollicités en 2021 dans ce contexte.

CHAPITRE VI.
AVIS

L'article 33 de la Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (L.Contrôle) stipule que le Comité « *ne peut rendre un avis sur un projet de loi, d'arrêté royal, de circulaire, ou sur des documents de toutes natures exprimant les orientations politiques des ministres compétents, qu'à la demande de la Chambre des représentants ou du Ministre compétent* ».

En 2021, l'avis du Comité permanent R a été sollicité à six reprises.[281] La Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières Administratives a adressé deux demandes d'avis au Comité concernant la création d'une agence fédérale de renseignement (VI.1.) et concernant les incriminations visant à promouvoir la résilience démocratique (VI.5.). La Chambre des représentants a également introduit une demande d'avis auprès du Comité (sur l'obligation de notification (VI.2.)). Le ministre de la Justice a, à son tour, sollicité deux fois l'avis du Comité (sur la rétention des données (VI.3.) et sur les modifications de la Loi organique des services de renseignements (VI.4.)). Enfin, conjointement avec le Comité permanent P, un avis a été émis à la demande du ministre de l'Intérieur (relatif aux modifications de la L.OCAM (VI.6.)).[282] Les avis sont résumés, en ordre chronologique, dans le présent chapitre. Ils sont consultables, dans leur intégralité, sur le site internet du Comité.[283]

Par ailleurs, le Comité doit rendre des avis en tant qu'autorité de contrôle compétente (ACC) dans le cadre des traitements de données à caractère personnel ainsi que dans le cadre de la réglementation relative aux banques de données communes, et ce conjointement avec l'Organe de contrôle de l'information policière (C.O.C.). Ces deux compétences d'avis sont traitées respectivement au Chapitre IV. et au Chapitre V.

---

281 Le Comité est de plus en plus sollicité sur la base de l'article 33 L.Contrôle; le temps consacré à la formulation d'avis a, par conséquent, considérablement augmenté.

282 Les Comités permanents R et P ont formulé cet avis tant en leur qualité d'organes de contrôle de l'OCAM en vertu de la L.Contrôle qu'en leur qualité d'autorités de protection des données à l'égard des traitements de données à caractère personnel par l'OCAM.

283 www.comiteri.be.

VI.1. AVIS RELATIF À LA CRÉATION D'UNE AGENCE FÉDÉRALE DU RENSEIGNEMENT

Le Comité permanent R a été sollicité en décembre 2020 par la Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives de la Chambre des représentants pour rendre un avis dans le cadre de l'examen de la proposition de résolution visant à la création d'une agence fédérale du renseignement.[284]

Cette proposition de résolution visait à demander au gouvernement fédéral de :

- procéder à un audit des services de renseignement et d'un service de la police fédérale (DR3) portant sur la circulation de l'information au sein et entre ces services ;
- créer, sur la base de cet audit, une agence nationale de renseignement regroupant les services de renseignement existants sous la tutelle du Premier ministre ;
- mettre à la disposition de cette agence des moyens humains et techniques nécessaires à l'exécution de ses missions.

Dans son avis, le Comité permanent R s'est dit prêt à participer (en collaboration avec le Comité permanent P et l'Organe de contrôle de l'information policière (C.O.C.) également compétents) à cet audit, dont la portée se devait cependant d'être mieux précisée. À cet égard, il a rappelé la pluralité des acteurs et partenaires belges compétents dans le cadre de la lutte contre la menace terroriste. Il a également souligné qu'il était prématuré de tirer des conclusions quant à la nécessité de créer une nouvelle institution regroupant un seul service de renseignement et un seul service de la Police fédérale (et des moyens à mettre à disposition de cette agence) sans disposer des résultats de l'audit sollicité.

VI.2. AVIS RELATIF À L'INSTAURATION D'UNE OBLIGATION DE NOTIFICATION POUR LES SERVICES DE RENSEIGNEMENT

Fin janvier 2021, une proposition de loi a été déposée visant à modifier la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) en vue de l'instauration d'une obligation de notification active pour certaines méthodes spécifiques de collecte de données.[285] Cette proposition de loi visait

---

[284] Ce projet de résolution a été déposé à la Chambre en septembre 2019. En avril 2022, il était toujours pendant (*Doc.Parl.* Chambre 2019-2020, 55-0287).

[285] *Doc.Parl.* Chambre 2020-2021, 55-1763/001. Le Comité a reçu la demande d'avis de la Chambre des représentants le 6 mai 2021 et a rendu son avis le 31 mai 2021. Le président du Comité a présenté cet avis en Commission Justice le 2 juin 2021. En avril 2022, le projet était toujours pendant à la Chambre.

à introduire, dans le chef des services de renseignement belges, d'une part et principalement une obligation de notification active, et d'autre, une obligation de notification passive.

Une *obligation de notification active* signifie que, sous certaines conditions, les services de renseignement informent de leur propre chef une personne visée qu'elle a fait l'objet d'une méthode de renseignement donnée dans le passé.

Une *obligation de notification passive* signifie qu'à la requête de toute personne ayant un intérêt personnel et légitime qui relève de la juridiction belge, le service de renseignement concerné doit informer celle-ci, moyennant certaines conditions et modalités, qu'elle a fait l'objet d'une méthode de renseignement dans le passé.

VI.2.1. LA NOTIFICATION ACTIVE

La question de savoir si un pays européen est tenu d'instaurer une obligation de notification active, trouve sa réponse dans la Convention européenne des droits de l'homme (CEDH), la jurisprudence de la Cour européenne des droits de l'homme, la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (modernisée en Convention 108+)[286] et, le cas échéant, dans la Constitution et la jurisprudence applicable de la Cour constitutionnelle du pays concerné.

Le Comité a constaté dans son avis que ni la CEDH ni la jurisprudence de la Cour européenne ne contenaient une obligation explicite pour les États parties d'instaurer à tout moment une telle obligation active de notification. Selon la Cour, le poids d'une telle obligation doit être mis en balance avec l'ensemble des garanties juridiques existantes. C'est donc l'ensemble des règles pertinentes du droit national, y compris celles régissant la transparence à l'égard de la personne concernée, qui doit être évalué.

S'appuyant sur deux arrêts de la Cour constitutionnelle[287] et sur la jurisprudence de la Cour européenne, l'exposé des motifs de la proposition de loi indiquait qu'il était nécessaire d'introduire la notification active. Le Comité a cependant estimé

---

[286] Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel Convention 108), amendée par le Protocole n° 223 du 18 mai 2018 (Convention 108+). Lorsque l'avis a été remis, la Convention 108+ n'était pas encore en vigueur en Belgique (raison pour laquelle le « + » a été mis entre parenthèses dans la suite des développements). Voir https://www.coe.int/fr/web/data-protection/convention108-and-protocol.

[287] Une obligation de notification avait déjà été introduite en 2010 et 2017 par le législateur à l'article 2 § 3 L. R&S. La Cour constitutionnelle a cependant annulé l'article 2 § 3 L. R&S à deux reprises, considérant que les garanties juridiques procédurales existantes étaient insuffisantes pour justifier l'absence d'une obligation de notification active pour les services de renseignement.

que cette affirmation devait être nuancée dès lors que depuis les lois de 2010 et 2017[288], le législateur avait mis en place de nouvelles garanties procédurales.[289]

La protection juridique des citoyens – et notamment le droit à la vie privée, le droit à la protection des données à caractère personnel et le droit à un recours effectif – a été largement modifiée et rehaussée grâce à la Loi du 30 mars 2018 relative à la protection des personnes physiques à l'égard des traitements des données (LPD). Avec cette loi, le législateur a non seulement élargi et clarifié le cadre réglementaire des services de renseignement (articles 72 à 104 LPD[290]), mais il a également introduit un mécanisme de contrôle correctif renforcé en désignant le Comité permanent R comme l'autorité compétente en matière de protection des données (DPA) dans le domaine de la 'sécurité nationale'.[291] Depuis la LPD, tout acte de collecte, de traitement, d'analyse et de transmission d'informations, ainsi que toute conservation de données, est soumis au contrôle correctif du Comité lorsqu'il s'agit de traitement de données à caractère personnel.[292] Ce qui est significatif à la lumière du droit à un recours effectif, c'est que, contrairement à une plainte MRD[293] dans laquelle le requérant doit énoncer ses griefs et démontrer son intérêt personnel et légitime, aucune condition formelle de ce type n'est requise lors de l'introduction de la demande visée à l'article 51/2 de la L.Contrôle : « *Pour être recevable, la requête est écrite, datée, signée et motivée, et justifier de l'identité de la personne concernée* ». Et dans la pratique, le Comité adopte une approche très souple quant à l'exigence de motivation. Contrairement à la situation antérieure

---

288 Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité, *M.B.* 10 mars 2010 et Loi du 30 mars 2017 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal, *M.B.* 28 avril 2017.

289 En sus, le Comité a souhaité faire remarquer que ni l'exposé des motifs de la Loi du 30 mars 2017 ni la Cour constitutionnelle ne faisaient référence aux garanties procédurales prévues par la Loi du 11 avril 1994 relative à la publicité de l'administration (LPA). Pourtant la problématique de la notification active pourrait également être analysée dans le cadre du droit d'accès aux documents administratifs et aux informations des services de renseignement dès lors que, dans une certaine mesure, cette législation permet l'information de la personne concernée. Tant le Conseil d'État que la Commission d'accès aux documents administratifs ont en effet confirmé à maintes reprises que la LPA s'applique à la VSSE et au SGRS.

290 Le sous-titre 1er titre 3 de la LPD (artt. 72 à 104 LPD) règle le traitement des données à caractère personnel par la VSSE et le SGRS dans le cadre de l'exécution de leurs missions, à l'exception des traitements de données à caractère personnel dans le cadre de la Loi du 11 décembre 1998 relative à la Classification. Ce dernier point est traité au sous-titre 3 du titre 3 de la LDP (artt. 106 à 137 LPD).

291 COMITÉ PERMANENT R, *Rapport d'activités 2019*, 75-80.

292 Compte tenu de l'interprétation large donnée par les traités à la notion de 'traitement de données à caractère personnel' (*cf.* article 8 de la CEDH, *i.o.* Convention n° 108(+)) tous les traitements de données à caractère personnel effectués par les services de renseignement sont soumis au contrôle APD du Comité. En sa qualité d'autorité de protection des données, le Comité permanent R agit soit d'initiative, soit à la demande d'une autre autorité de protection de données, ou encore à la requête de toute personne concernée.

293 Visé à l'article 43/4, alinéa 1er, troisième tiret L.R&S.

à la Loi sur la protection des données, le droit à un recours effectif est donc sensiblement amélioré.

Le Comité a indiqué que le renforcement de ses attributions consécutif à l'adoption de la LPD en 2018, conjugué à la mise en place d'un système de notification passive[294] prévue par ladite proposition, permettait à ses yeux de rencontrer l'exigence de transparence issue du droit international. À la lumière de cette constatation, le Comité a considéré que le législateur fédéral n'avait pas d'obligation conventionnelle d'instaurer une obligation de notification active, pour autant que la proposition introduise bien une obligation de notification passive tenant compte des commentaires du Comité (*infra*).

Néanmoins, le Comité a souhaité ajouter et souligner que le législateur fédéral était libre d'instaurer un tel mécanisme.[295] Et dans l'éventualité où le législateur faisait ce choix, le Comité a formulé un certain nombre de commentaires sur les différents articles relatifs à l'obligation de notification active. Les remarques avaient notamment trait :

- au choix (inexpliqué) opéré dans la proposition de loi de limiter le champ d'application à certaines MRD ;
- à la différence observée avec l'obligation de notification active qui existe dans la procédure pénale (article 90*novies* CIC) ;
- aux motifs d'exception qui devraient s'aligner davantage sur ceux déjà contenus dans plusieurs réglementations (LPA, L.C&HS, L.R&S et L.Organe de recours) ;
- aux personnes à notifier ;
- au délai de notification ;
- à l'autorité de contrôle, le Comité étant d'avis qu'une instance de contrôle suffit.

Par ailleurs, le Comité a recommandé que des moyens supplémentaires soient alloués aux deux services de renseignement en cas d'instauration d'une telle obligation. Sans ces ressources supplémentaires, l'introduction d'une telle obligation de notification active affecterait les priorités stratégiques et opérationnelles de la VSSE et du SGRS.

VI.2.2. LA NOTIFICATION PASSIVE

Tout en accueillant positivement la proposition de réintroduire la notification passive, le Comité a relevé que différents systèmes, compétences et procédures existaient déjà en matière de transparence des informations en possession des services de renseignement. À cet égard, le Comité a souligné que les possibilités d'action étaient complexes à cerner et à mettre en œuvre pour le citoyen et que le

294 Prenant en considération les observations formulées dans l'avis rendu.

295 Le Comité a relevé dans son avis qu'une décision d'introduire (une certaine forme) d'obligation de notification active avait été prise dans 6 des 47 États membres du Conseil de l'Europe.

choix d'une procédure avait actuellement un impact sur ses possibilités d'accès (ou non) à de l'information. Aux yeux du Comité, une harmonisation des procédures d'accès à l'information et des exceptions à la communication d'information – et donc une harmonisation du résultat des différentes procédures – était dès lors souhaitable.

Dans le même ordre d'idées, le Comité a souhaité attirer l'attention du législateur sur la nécessité d'expliciter et de préciser davantage dans l'exposé des motifs la manière dont le système de notification passive s'articulerait avec les procédures existantes.

VI.3. AVIS RELATIF À LA RÉTENTION DES DONNÉES

Le Comité permanent R a été sollicité par le ministre de la Justice pour rendre un avis sur le projet de loi 'relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités' (ci-après : le projet de loi).[296] [297] Suite à l'annulation par la Cour constitutionnelle des articles 2, b), 3 à 11 et 14 de la Loi du 29 mai 2016 'relative à la collecte et à la conservation des données dans le secteur des communications électroniques'[298], le projet de loi visait à instaurer un système de conservation des données de communication qui respecte les exigences imposées par la Cour de justice de l'Union européenne (CJUE). Pour ce faire, il entendait modifier plusieurs lois parmi lesquelles la Loi du 13 juin 2005 relative aux communications électroniques (Loi LCE) et la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S).

Le Comité permanent R a discuté, dans son avis, les modifications proposées dans la L.R&S, et les modifications proposées dans la Loi LCE relevant de sa compétence.[299]

---

296 Le Comité permanent R a reçu la demande le 7 mai 2021 et a rendu son avis le 15 juin 2021.

297 L'avant-projet a été approuvé en deuxième lecture par le Conseil des ministres en décembre 2021 et déposé à la Chambre en mars 2022. Toujours en mars 2022, 18 amendements ont été approuvés par le Conseil des ministres (suite à l'arrêt n° 158/2021 pris par la Cour constitutionnelle le 18 novembre 2021). Les avis du Conseil d'État et de l'APD sur ces amendements ont été sollicités. L'APD a remis un avis le 1er avril 2022 (Voir avis n°66/2022 de l'APD).

298 Cette loi avait été annulée en raison de sa contrariété avec le droit européen et la jurisprudence de la CJUE.

299 Le Comité ne s'est pas prononcé quant à la question de savoir si les modifications apportées à la Loi LCE par le projet rencontraient ou non les exigences consacrées dans les jurisprudences de la CJUE et de la Cour constitutionnelle belge. Cf. l'avis de l'autorité de protection des données rendue sur le projet de loi https://www.autoriteprotectiondonnees.be/publications/avis-n-108-2021.pdf

VI.3.1. MODIFICATIONS À LA LOI ORGANIQUE DES SERVICES DE RENSEIGNEMENT

VI.3.1.1. Conservation ciblée des données de trafic et de localisation

Le gouvernement proposait d'inclure dans la L.R&S une nouvelle méthode ordinaire de conservation ciblée des données de trafic et de localisation dans le secteur des communications électroniques.

Le Comité a relevé une divergence inexpliquée dans le niveau de protection juridique qu'offrait le projet de loi dans le cadre de la conservation ciblée selon que cette dernière était opérée dans le cadre d'une procédure pénale ou d'une procédure de renseignement.

Il notait par ailleurs que le mécanisme de contrôle proposé dans le cadre de la procédure de renseignement – à savoir une notification mensuelle des méthodes utilisées (donc après la mise en œuvre de plusieurs méthodes) – n'était pas suffisant et ne répondait pas à l'exigence de la CJUE qui estime que la conservation ciblée des données de trafic et de localisation nécessite que la décision de l'autorité compétente soit soumise à un contrôle juridictionnel effectif.

Le Comité a également pointé un pouvoir de délégation inapproprié dans le cadre de cette nouvelle méthode ordinaire de conservation ciblée qui concerne les données de trafic et de localisation relatives aux communications électroniques. Le gouvernement proposait que le pouvoir de réquisition de ces données puisse être exercé par « *le dirigeant de service ou son délégué* ». À l'instar de la Cour constitutionnelle et de la Cour EDH, le Comité est d'avis que de telles données sont très intrusives. Il ne perçoit pas de justification à l'instauration d'un pouvoir de délégation supplémentaire que celui déjà inscrit dans la L.R&S[300], et a invité par conséquent le gouvernement à motiver ce choix.

VI.3.1.2. Accès aux données de trafic et de localisation

Le projet de loi visait à rétablir l'article 18/8 L.R&S, qui a été en grande partie annulé par la Cour constitutionnelle[301] et qui réglait l'accès aux données relatives au trafic et à la localisation des communications électroniques par les services de renseignement.

Le Comité a rappelé que la Cour constitutionnelle avait annulé l'intégralité de l'article 18/8 L.R&S. De l'avis du Comité, il était prématuré de conclure que seule

---

300 La définition juridique de la notion de dirigeant du service contient déjà un pouvoir de délégation : en cas d'empêchement de l'Administrateur général de la VSSE ou du Chef du SGRS, les dirigeants des service respectifs ont la possibilité de déléguer leur pouvoir de décision à, respectivement, l'Administrateur général ou au chef de service faisant fonction. Cette délégation n'est pas limitée à l'Administrateur général adjoint de la VSSE et au Chef adjoint du SGRS. En cas d'empêchement de ces derniers, une nouvelle délégation peut être faite à un niveau inférieur de la hiérarchie.

301 C.C., 22 avril 2021, n° 57/2021.

l'annulation du paragraphe 2 s'imposait à la lumière de jurisprudence de la Cour constitutionnelle et de la Cour EDH. Ce sont les garanties juridiques procédurales dans leur ensemble qui doivent être prises en considération.

VI.3.1.3. Conservation généralisée et indifférenciée des données de trafic et de localisation

Le projet de loi proposait d'inscrire dans la L.R&S une nouvelle méthode exceptionnelle dans le cadre de la conservation des données relatives au trafic et à la localisation dans le secteur des communications électroniques lorsqu'il existe une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Dans ce cas, le projet prévoyait la possibilité pour les services de renseignement de requérir le concours des opérateurs pour procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traités par eux.

Le Comité souscrivait pleinement à la proposition de soumettre l'utilisation de cette compétence à tous les mécanismes de contrôle inhérents aux méthodes exceptionnelles.

Il recommandait de renforcer le lien entre la disposition réglant l'accès et celle réglant la conservation généralisée. Tel que le projet était rédigé, il était possible qu'une menace bien définie (par exemple, le terrorisme) puisse justifier l'imposition d'une conservation généralisée et indifférenciée aux opérateurs de télécommunications, sans aucune limitation ultérieure, et que l'accès à ces données puisse également être utilisé à d'autres fins (par exemple, dans le cadre de la lutte contre d'autres menaces).

Par ailleurs, dans l'exposé des motifs, il était indiqué que : « *l'autorisation prise par le dirigeant du service concerné de mettre en œuvre cette méthode exceptionnelle est transmise au ministre compétent pour information. Il convient de préciser que le but est donc d'informer le ministre compétent qu'une conservation indifférenciée est déclenchée* ».[302] Le Comité recommandait que le ministre concerné soit informé non seulement de 'l'autorisation' définitive du dirigeant du service, mais aussi du 'projet d'autorisation'. Ni la notification du projet d'autorisation ni la notification de l'autorisation ne sont prévues dans la procédure MRD pour les méthodes exceptionnelles. Toutefois, le Comité estimait que si les services de renseignement ordonnent aux opérateurs de télécommunications une conservation généralisée et indifférenciée[303] des données de trafic et de localisation, l'impact en termes

[302] Avant-projet de Loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités, pp.111-112.

[303] Par opposition aux autres méthodes exceptionnelles qui sont ciblées (cf. art. 18/10, §2, 2° L.R&S).

d'ingérence dans la vie privée des citoyens belges et des résidents sur le territoire belge est tel que pareilles exigences de forme divergentes se justifient.[304]

Le Comité a également pointé l'absence de motivation justifiant des délais de conservation des données[305] et de rapportage[306] différents de ceux d'application dans le cadre des méthodes exceptionnelles.

Le Comité recommandait encore de clarifier le rapport entre cette mesure et le régime de protection particulier pour les avocats, les médecins et les journalistes prévu par la L.R&S.[307]

VI.3.1.4. Notification obligatoire des décisions du Comité aux opérateurs

Le Comité recommandait aussi de créer une obligation pour les services de renseignement d'informer les opérateurs concernés lorsque le Comité permanent R avait ordonné la cessation d'une conservation généralisée et indifférenciée ou d'une conservation ciblée.

VI.3.2. MODIFICATIONS À LA LOI TÉLÉCOM (LCE)

Le Comité a également formulé plusieurs remarques quant aux modifications proposées dans la Loi LCE. Tout d'abord, le projet de loi proposait, dans le cadre de la conservation ciblée de données en cas de menace grave, réelle et actuelle pour la sécurité nationale, que celle-ci s'opère pour toutes les 'zones' dont le niveau de la menace évaluée par l'OCAM soit au moins de niveau 3, et aussi longtemps qu'un niveau 3 perdure pour ces 'zones'. Le Comité invitait à préciser la notion de 'zones' afin de clarifier à quoi celles-ci se référaient.

Le projet chargeait les services de renseignement d'établir une liste annuelle « *(d)es bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé* », devant être approuvée par le Conseil national

---

304 La notification du projet d'autorisation au ministre compétent n'aurait pas pour but de porter le pouvoir décisionnel au niveau ministériel, mais de rendre obligatoire l'information du gouvernement sur le fait que, selon le service de renseignement concerné, il existe un danger pour la sécurité nationale d'un niveau si élevé qu'une mesure aussi intrusive de conservation généralisée et indifférenciée des données de communication en question semble justifiée.

305 Le projet proposait une durée de conservation de maximum six mois au lieu de deux mois prolongeable.

306 Le projet proposait un rapport tous les deux mois, ce qui s'écarte du rapportage une fois toutes les deux semaines qui est imposé pour les autres méthodes exceptionnelles.

307 En vertu de l'article 18/9, § 4 L.R&S, des méthodes exceptionnelles ne peuvent être utilisées contre l'une de ces professions protégées ou, entre autres, contre les moyens de communication utilisés à des fins professionnelles, que si le service de renseignement dispose au préalable d'indices sérieux révélant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement d'une menace potentielle grave. Le cas échéant, il y a lieu de suivre une procédure particulière.

de sécurité. À cet égard, le Comité a rappelé l'existence du Plan d'action du gouvernement fédéral pour la sauvegarde du potentiel scientifique et économique[308]. Ce plan d'action contient également une liste d'entités. Le Comité constatait que la liste établie en 2007 n'avait pas été actualisée depuis et se demandait, par conséquent, si la mise à jour annuelle prévue par le projet de loi était réaliste.

Le Comité relevait encore que le projet ne prévoyait pas d'obligation de notification aux autorités de protection des données vis-à-vis de l'OCAM (à savoir le Comité permanent R et le Comité permanent P) en cas de conservation géographique ciblée effectuée sur la base du niveau de menace général tel que déterminé par l'OCAM. Il recommandait d'établir une obligation de notification pour le Comité permanent R et d'interroger le Comité permanent P à cet égard.

VI.4. AVIS CONCERNANT L'AVANT-PROJET DE LOI MODIFIANT LA LOI ORGANIQUE DES SERVICES DE RENSEIGNEMENT

À la demande du ministre de la Justice, le Comité permanent R a rendu un avis concernant l'avant-projet de loi 'modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité'.[309] [310] Le projet de loi prévoyait notamment, pour les agents des services de renseignement, un élargissement des possibilités de commettre des infractions ainsi qu'une procédure spécifique pour l'utilisation des identités fictives. Il introduisait également la possibilité pour les sources humaines de commettre certaines infractions ainsi que la possibilité de réaliser des MRD pour contrôler la fiabilité d'une soucre. Le projet visait également à introduire une nouvelle compétence pour le SGRS en cas de crise nationale de cybersécurité. Un remaniement de la méthode de collecte déjà existante auprès des institutions bancaires et financières était également proposé.

VI.4.1. UNE RÉGLEMENTATION TROP COMPLEXE

De manière générale, le Comité constatait dans son avis que les modifications législatives proposées rendaient beaucoup plus complexe et incohérente la réglementation qui s'applique à la VSSE et au SGRS. Le Comité déplorait que le

---

308 Ce plan a été approuvé le 16 mars 2007 par le Comité ministériel du renseignement et de la sécurité (aujourd'hui, le Conseil national de sécurité).

309 Le ministre a fait sa demande le 31 mai 2021; le Comité a rendu son avis le 15 juin 2021. C'était le deuxième avis du Comité dans ce contexte. À la demande du ministre de la Justice, le Comité avait déjà rendu un avis le 16 novembre 2018 sur un projet de loi dans lequel les mesures proposées étaient (en grande partie) les mêmes.

310 En avril 2022, cet avant-projet n'avait pas (encore) été approuvé en deuxième lecture par le Conseil des ministres.

projet de loi s'inscrivait dans l'évolution de ces dernières années d'abandonner la structure logique - mise en place par le législateur MRD en 2010 - dans la L.R&S en ce qui concerne les compétences (d'enquête) des services de renseignement.
Le Comité notait en outre que certains choix opérés dans le projet de loi étaient inutilement compliqués et incomplets, ce qui n'allait pas favoriser, selon le Comité, une bonne application de la législation en question.

VI.4.2. CYBERSÉCURITÉ - MISSION DU SGRS

Le projet de loi conférait au SGRS la nouvelle compétence de « *neutraliser, dans le cadre d'une crise nationale de cybersécurité, une cyberattaque de systèmes informatiques et de communications non gérés par la Défense et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit international* ».
Le Comité constatait que cette nouvelle mission complétait la mission de cybersécurité existante[311], en offrant la possibilité au SGRS d'agir contre une cyberattaque menée contre les systèmes informatiques et de communications qui ne sont pas gérés par le ministre de la Défense. La compétence matérielle du SGRS dans le cadre de cette mission, était déterminée par la proposition de définition du concept de « *crise nationale de cybersécurité* », à savoir « *tout incident de cybersécurité qui, par sa nature ou ses conséquences :*
- *menace les intérêts vitaux du pays ou les besoins essentiels de la population ;*
- *requiert des décisions urgentes ;*
- *et demande une action coordonnée de plusieurs départements et organismes* ».[312]

De l'avis du Comité, les entités à protéger étaient définies de manière trop large dans le projet de loi, l'expression 'les intérêts vitaux du pays ou les besoins essentiels de la population' n'étant pas suffisament définie. Le Comité recommandait de délimiter le champ d'action aux 'infrastructures critiques' (cf. la Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques).

Outre la compétence de 'neutraliser' une cyberattaque, le projet octroyait au SGRS la compétence de réagir par 'une propre cyberattaque'. Le Comité s'interrogeait, dans son avis, sur le cadre juridique à respecter dans la mise en œuvre d'un tel pouvoir d'attaque qui s'inscrit dans le droit de la guerre. Des

311 Cette compétence est définie à l'article l'article 11, § 1er, 2° L.R&S et permet SGRS d'agir contre une cyberattaque de systèmes informatiques et de communications gérés par le ministre de la Défense.

312 L'exposé des motifs précisait que la définition du mot « crise » avait été reprise de l'article 2 de l'Arrêté royal du 18 avril 1988' portant création du Centre gouvernemental de Coordination et de Crise'.

éclaircissements quant la manière dont le droit de la guerre s'articulerait dans pareil cas avec le droit penal étaient nécessaires.[313]

VI.4.3. LA COMMISSION D'INFRACTIONS D'APPUI

VI.4.3.1. Généralités

Le projet de loi permettait la commission d'infractions en appui à l'exécution de différents types de missions de la VSSE et du SGRS. Le Comité recommandait de supprimer la possibilité de commettre des infractions par le SGRS dans le cadre de ses missions du maintien de la sécurité militaire et la protection du secret. Le Comité n'en voyait pas la nécessité, et aucun motif n'était développé pour en justifier le besoin.

Le projet de loi contenait également une liste d'infractions ne pouvant pas être commises par les agents des services de renseignement ou par les sources humaines (HUMINT). Le Comité constatait que cette liste n'était pas exhaustive et il proposait d'y ajouter plusieurs infractions.

Par ailleurs, le Comité déplorait que le projet de loi ne permettait pas à la Commission BIM d'imposer une interdiction d'exploitation et une ordonnance de destruction des données collectées lorsque des infractions d'appui étaient commises illégalement dans le cadre de l'utilisation de méthodes ordinaires. Il recommandait de donner à la Commission BIM les mêmes compétences de contrôle et de sanction que celles dont elle dispose pour le contrôle des méthodes exceptionnelles (cf. article 18/10, § 6 L.R&S). En conséquence, la 'commission d'infractions' ne deviendrait pas une méthode exceptionnelle, mais elle serait contrôlée comme les méthodes exceptionnelles. Le même niveau de protection juridique s'appliquerait donc.

VI.4.3.2. Lacune dans la procédure pénale

Le Comité attirait également l'attention sur l'absence d'une procédure de contrôle sur la régularité de l'enquête de renseignement au cours de la procédure pénale, à l'instar de la mission de contrôle dont est animée la chambre des mises en accusation dans l'enquête judiciaire (cf. art. 235*bis* et suiv. CIC). En dehors d'une

313 Sachant qu'une cyberattaque contre les infrastructures IT belges constitue en soi une infraction, la question se posait de savoir si une telle cyberattaque n'interfèrerait pas avec les missions judiciaires. Une situation dans laquelle une infraction avec une dimension purement nationale serait commise devrait être traitée par le droit pénal.

procédure à portée limitée[314], il n'existe pas de procédure comparable. Ce contrôle est pourtant nécessaire, puisqu'un dossier pénal peut également contenir des notes des services de renseignement.

Le Comité recommandait par conséquent de généraliser la 'procédure d'avis préjudiciel en matière pénale'. Les tribunaux pénaux devraient ainsi avoir la possibilité d'interroger le Comité permanent R sur la légalité des données de renseignement contenues dans le dossier pénal.

VI.4.3.3. La commission d'infractions par des agents

Afin d'assurer le suivi de la commission d'une infraction ayant été autorisée par la Commission BIM pour un agent, le Comité recommandait que soit indiqué, dans la demande écrite d'autorisation, le nom de la personne chargée du contrôle de l'utilisation de cette mesure.[315]

Pour garantir la protection des agents, le Comité recommandait également de prévoir la possibilité d'un recours juridictionnel auprès du Comité contre une décision négative de la Commission BIM devant statuer – dans le cadre d'une procédure exceptionnelle lors de laquelle elle n'avait pas été invitée *a priori* à autoriser la commission d'infraction – sur le caractère imprévisible et strictement nécessaire de l'infraction commise.

VI.4.3.4. La commission d'infractions par des informateurs

Quant aux infractions commises par des sources humaines, le Comité recommandait de préciser que celles-ci n'étaient autorisées que dans le cadre des missions de renseignement. Il estimait ensuite que le champ d'application matériel de cette exemption de peine n'était pas suffisamment clair vu l'absence de définition légale du concept de 'sources humaines'.

Pour assurer un contrôle efficace, le Comité recommandait que soit inscrit, dans la demande d'autorisation, le nom de l'agent traitant de la source humaine concernée. Le Comité estimait également que les organes de contrôle concernés devaient être habilités à prendre connaissance de l'identité de l'informateur.[316]

---

314 Il s'agit de la procédure dite « d'avis préjudiciel » (cf. art. 131*bis*, 189*quater* et 279*bis* CIC) dans laquelle un tribunal pénal peut interroger le Comité permanent R quant à la régularité des méthodes qui ont conduit à la rédaction d'un « procès-verbal non classifié » (cf. art. 19/1 L.R&S). Ce procès-verbal est établi par la Commission BIM lorsque des indices d'infractions sont mis en évidence par l'utilisation de MRD.

315 Le Comité admet qu'il n'est pas toujours possible de connaître à l'avance le nom de l'agent chargé de mettre en œuvre une méthode de renseignement ou une mesure de protection et d'appui. Mais ce n'est pas le cas de la personne chargée du suivi de la mesure.

316 Donner à un informateur (c'est-à-dire une personne privée) l'autorisation de commettre des délits sans que la Commission BIM ne sache à qui cette autorisation est donnée rend impossible un contrôle efficace.

VI.4.3.5. Dommages subis ou causés par une source humaine

Le projet instaurait une procédure – ainsi qu'un système d'indemnisation – pour régler les cas de dommages subis ou causés par une source humaine pendant sa mission. Le Comité soulignait le manque de clarté dans la description de la procédure.

VI.4.3.6. Protection juridique insuffisante de la source humaine

Le Comité constatait que le projet de loi ne prévoyait pas un degré adéquat de protection juridique pour la source humaine ayant obtenu l'autorisation de commettre certaines infractions. La question de savoir comment les autorités judiciaires concernées pouvaient savoir avec certitude qu'une personne verbalisée avait été autorisée par la Commission BIM à commettre certaines infractions demeurait sans réponse.[317] Le Comité recommandait diverses mesures pour y remédier.[318]

VI.4.4. IDENTITÉ ET QUALITÉ FICTIVES COMME MESURE D'APPUI À UNE MÉTHODE DE RENSEIGNEMENT OU UNIQUEMENT POUR DES RAISONS DE SÉCURITÉ

Le projet de loi modifiait la procédure – établie à l'article 13/2 L.R&S – pour la création et l'utilisation d'une identité fictive et créait une nouvelle compétence en matière d'utilisation d'une identité fictive à des fins de collecte d'informations.

Le Comité recommandait de permettre à la Commission BIM de réaliser un contrôle dans tous les cas de figure où celle-ci est d'avis que l'identité fictive est utilisée pour la collecte d'informations (et ce, même si le service concerné avance d'autres motifs pour justifier le recours à l'identité fictive). Le Comité invitait également à préciser dans la loi la signification exacte de 'l'identité fictive' et de la 'qualité fictive'.[319]

---

317 Ceci est problématique puisque le parquet, la juridiction d'instruction ou, en dernière instance, la juridiction de jugement sont les autorités compétentes pour juger de l'existence concrète d'une exemption de peine dans le chef de la personne verbalisée.

318 Telles que la possibilité pour la Commission BIM de rédiger, dans certains cas, un acte décrivant son autorisation pour la commission de certaines infractions ; la conclusion d'un protocole d'accord entre les services de renseignement, la Commission BIM et le Collège de procureurs généraux visant à garantir un canal de communication effectif entre ces acteurs relatif à cette question.

319 Le Comité s'interrogeait notamment sur le fait de savoir si le simple fait d'omettre délibérément de révéler à un interlocuteur la qualité d'un membre d'un service de renseignement lors de la collecte de données revenait à utiliser une qualité fictive.

VI.4.5. INFILTRATION DANS LE MONDE RÉEL ET VIRTUEL

Le projet de loi optait pour une exécution indirecte du contrôle de la compétence d'infiltration via le contrôle de la commission d'infractions et/ou l'utilisation d'une identité fictive. La procédure qui en découlait était inutilement compliquée, incomplète et ne répondait en aucun cas aux garanties juridiques nécessaires dans le cadre d'un pouvoir d'investigation d'une telle ampleur. Un avis négatif a donc été rendu par le Comité quant à l'exécution de ce contrôle. Il estimait en effet que le projet de loi ne répondait pas aux exigences fixées par la Commission d'enquête parlementaire « Attentats » en termes de protection juridique.[320]

Le projet de loi considérait cette nouvelle compétence comme une méthode ordinaire. Compte tenu de la manière dont l'infiltration est organisée dans la procédure pénale, le Comité recommandait de considérer 'l'infiltration dans le monde réel' comme une méthode exceptionnelle et 'l'infiltration dans le monde virtuel' comme une méthode spécifique.

Par ailleurs, le Comité constatait que la procédure d'autorisation prévue donnait l'impression – erronée – d'être identique à celle prévue pour les méthodes exceptionnelles. Divers mécanismes de contrôle applicables aux méthodes exceptionnelles n'étaient pas d'application.

Considérer le pouvoir d'infiltration comme une MRD – comme l'a suggéré le Comité dans son avis – présenterait également l'avantage de rendre possible un contrôle structuré des résultats d'enquête par la Commission BIM.[321]

VI.4.6. MÉTHODES ORDINAIRES PLUS

Dans son avis, le Comité soulignait que les garanties procédurales pour les méthodes ordinaires (MPLUS) plus n'étaient pas suffisantes et que le contrôle n'offrait pas un niveau de protection juridique adéquat. Il recommandait, par conséquent, un renforcement du contrôle des méthodes ordinaires plus (MPLUS), en traitant toutes les MPLUS de la même manière et en créant une obligation pour les services de renseignement de faire précéder chaque utilisation d'une MPLUS d'une décision

---

320 L'exposé des motifs faisait à juste titre référence au Troisième rapport intérmédiaire de la Commission d'enquête parlementaire sur les attentats terroristes, qui recommande la création d'une compétence d'infiltration pour les services de renseignement. Mais la recommandation indique également que « *(l)a réglementation légale à adopter en la matière devra toutefois prévoir les garanties nécessaires, tant en termes de protection juridique des citoyens qu'en termes de sécurité des agents de la VSSE chargés de missions d'infiltration* ». *Doc. Parl.*, Chambre, 2016-17, n° 54-1752/008.

321 Si par le passé, la procédure d'autorisation MRD n'était peut-être pas suffisamment adaptée à l'exercice d'un pouvoir d'infiltration, le législateur a depuis créé un certain nombre d'instruments dans la L.R&S pour passer outre ces obstacles.

écrite et motivée, et de communiquer chaque décision spontanément et dans les meilleurs délais au Comité.[322]

VI.4.7. RÉCLAMATION DE DONNÉES FINANCIÈRES

Le projet introduisait une nouvelle méthode ordinaire, créant une obligation pour les institutions financières, au sens large du terme, de coopérer afin d'identifier les produits ou services financiers dont dispose une personne ou, inversément, d'identifier quelle personne peut être liée à certains produits ou services financiers. Il s'agit pour l'heure d'une méthode exceptionnelle.

Le Comité recommandait de considérer cette méthode comme une méthode spécifique ne pouvant se rallier à la conclusion dans l'exposé des motifs selon laquelle « *le caractère intrusif d'une telle méthode est (...) faible à très faible* ».

VI.4.8. MOYENS EN PERSONNEL ET MOYENS FINANCIERS

Enfin, estimant que la mise en œuvre des différentes mesures élaborées dans le projet de loi créait non seulement une charge de travail supplémentaire pour les services de renseignement mais aussi pour les organes de contrôle concernés, le Comité plaidait pour que l'approbation du projet de loi soit accompagnée d'une augmentation des effectifs de la Commission BIM et du Comité permanent R.

VI.5. AVIS SUR DES PROPOSITIONS DE LOI À PROPOS D'INCRIMINATIONS VISANT À PROMOUVOIR LA RÉSILIENCE DÉMOCRATIQUE

En septembre 2021, le Comité permanent R a rendu un avis, à la demande du Président de la Commission de l'lnterieur, de la Sécurité, de la Migration et des Matières Administratives concernant trois propositions de loi:

– la proposition de loi incriminant l'appartenance ou la collaboration avec un groupement qui prône la discrimination ou la ségrégation ;

[322] En ne considérant pas les méthodes MPLUS comme des MRD, le législateur a choisi de ne pas faire effectuer de contrôle par la Commission BIM. Il a confié cette mission au Comité permanent R. Dans le cadre de son contrôle des MPLUS, le Comité, en tant que régulateur de la sécurité nationale en matière de protection des données dans ce domaine, a également le pouvoir de prendre des mesures correctrices contraignantes à l'égard de tous les traitements de données à caractère personnel effectués par les services de renseignement. En conséquence, le Comité a le pouvoir, par exemple, d'imposer une interdiction de traitement ou un effacement des données dans le cadre de son contrôle des MPLUS.

– la proposition de loi modifiant la loi du 29 juillet 1934 interdisant les milices privées en vue d'interdire les groupements non démocratiques ;
– la proposition de loi modifiant la loi du 29 juillet 1934 interdisant les milices privées, afin que les interdictions prévues par cette loi soient élargies pour viser les associations incitant à la haine, à la discrimination ou à la violence, et permettant leur dissolution par le pouvoir exécutif.[323] [324]

Les propositions législatives soumises à l'avis du Comité visaient à introduire de nouvelles dispositions pénales avec l'objectif général de promouvoir la résilience démocratique. Le Comité a limité son avis aux aspects des propositions de loi concernées qui ont ou peuvent avoir un impact sur les missions et le fonctionnement des services de renseignement et de sécurité.

VI.5.1. OBSERVATION PRÉALABLE

Le Comité a tout d'abord constaté que les actes punissables proposés pouvaient, dans certains cas, être également considérés comme des menaces pour la sécurité nationale, en ce qu'ils correspondent aux activités qui doivent être contrôlées par la VSSE, le SGRS et l'OCAM. De manière significative, l'incrimination de menaces à la sécurité nationale affecte le fonctionnement des services de renseignement et de sécurité.

En effet, la VSSE a notamment pour mission de rechercher, d'analyser et de traiter le renseignement relatif aux activités extrémistes qui menacent ou pourraient menacer la sécurité nationale. Le SGRS a lui aussi pour mission légale d'enquêter sur les activités extrémistes si celles-ci comportent un aspect militaire.

VI.5.2. COOPÉRATION ET ÉCHANGE D'INFORMATIONS AVEC LES ACTEURS JUDICIAIRES

Le Comité est d'avis qu'un élargissement (indirect) de l'arsenal pénal dans le cadre de la sécurité nationale accroit la nécessité de prévoir, de manière générale et formalisée, une coopération opérationnelle entre le Ministère Public, la Police judiciaire, la VSSE, le SGRS et l'OCAM.

Actuellement cette coopération opérationnelle et cet échange d'informations au sein de l'arrondissement judiciaire de Bruxelles sont largement organisés par

---

323 *Doc. parl.* Chambre 2021-2022, 55 n° 450/001, 55 n° 943/001 et 55 n° 2024/001.

324 Ces trois propositions de loi, encore pendantes à la Chambre en avril 2022, ont fait l'objet de débats en Commission Intérieur en juin et juillet 2021. Les rapports d'auditions ont été publiés en avril 2022.

le biais du système Joint Intelligence Centre (JIC)/ Joint Decision Centre (JDC)[325] en vue d'un échange et d'une évaluation commune des informations relatives à le menace terroriste. Dans son avis, le Comité recommandait d'examiner dans quelle mesure le système JIC/JDC devrait être étendu au suivi des menaces autres que le terrorisme, et plus particulièrement au suivi des infractions pénales proposées. Le Comité indiquait ensuite que le système JIC/JDC n'est applicable que dans l'arrondissement judiciaire de Bruxelles. Le Comité conseillait d'examiner l'utilité opérationnelle d'étendre ce système aux autres arrondissements et au suivi des infractions pénales proposées. Enfin, le Comité rappelait la recommandation de la Commission d'enquête parlementaire 'Attentats' de créer une Banque Carrefour de sécurité.

VI.5.3. COOPÉRATION ET ÉCHANGE D'INFORMATIONS AVEC LES ACTEURS ADMINISTRATIFS

Dans son avis, le Comité a également relevé que les mesures d'incrimination proposées affectent de manière significative la liberté d'expression, la liberté d'association et la liberté de réunion.

Le Comité a rappelé les obligations légales de la VSSE, du SGRS et de l'OCAM dans l'établissement des listes conjointes de 'phénomenes et de groupements à suivre' par la police : conformément à l'article 44/5, § 2 de la Loi sur la fonction de police (LFP), la VSSE, le SGRS et l'OCAM – en toute logique avec la Police fédérale – sont chargés d'établir annuellement pour le ministre de l'Intérieur 'une proposition conjointe' de listes de 'phénomènes de police administrative' et de 'groupements nationaux et internationaux susceptibles de porter atteinte à l'ordre public' et qui requièrent un suivi par la police. Le ministre de l'lntérieur établit ces listes annuellement. Dans son avis, le Comité recommandait d'examiner dans quelle mesure ces listes devaient être utilisées dans le suivi des organisations et groupements interdits visés dans les propositions de loi soumises pour avis.

[325] Le *Joint Intelligence Center* (JIC), composé de la Police judiciaire fédérale (PJF Bxl), du Service central de lutte contre le Terrorisme au sein de la Police fédérale (DJSOC/Terro), de la VSSE, du SGRS et de l'OCAM, est chargé de l'échange d'informations structurel dans le cadre de la lutte contre le terrorisme. Le JIC est également chargé d'évaluer conjointement tout nouveau renseignement relatif à la menace terroriste recueilli par l'un des services partenaires et de formuler une proposition de suivi approprié (suivi judiciaire/renseignement/autre). Le *Joint Decision Center* (JDC), composé des représentants du JIC, du ministère public et du directeur-coordinateur administratif de la police de Bruxelles, décide ensuite du suivi de manière collégiale.

VI.6. AVIS COMMUN SUR L'AVANT-PROJET DE LOI MODIFIANT LA LOI OCAM

En août 2021, les Comités permanents R et P ont été saisis par le ministre de l'Interieur et l'Autorité de protection des données afin de rendre un avis commun sur l'avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace (L.OCAM).[326] Sur certains points, le Comité permanent R a formulé des observations en son nom seul.

VI.6.1. EXTENSION DE LA LISTE DES SERVICES D'APPUI

L'avant-projet de loi visait tout d'abord à conférer un ancrage légal (dans la L.OCAM) aux quatre services publics désignés en tant que services d'appui de l'OCAM par l'Arrêté royal du 17 août 2018.[327]

En effet, alors que la L.OCAM prévoit que les services d'appui désignés par arrêté royal soient confirmés par une loi adoptée dans un delai d'un an à compter de la date d'entrée en vigueur de cet arrêté royal, les Comités permanents R et P observaient que cela n'avait pas été le cas. Ils notaient que l'avant-projet de loi venait remédier à cette situation, sans toutefois qu'il soit précisé dans l'exposé des motifs les raisons de l'intervention tardive du gouvernement.

Le Comité permanent R jugeait dès lors nécessaire de procéder à une évaluation de la possibilité juridique de désigner un service public comme service d'appui par le biais d'un arrêté royal. En effet, la question se pose de savoir si une évaluation de la menace établie par l'OCAM (et toute mesure fondée sur cette évaluation) est illégale si elle se fonde (entre autres) sur des informations provenant d'un service d'appui désigné par arrêté royal et transmises après le délai dans lequel cette désignation devait être légalement confirmée. Selon le Comité permanent R, il y a également lieu de s'interroger sur la question de savoir si le traitement de données à caractère personnel par un service d'appui qui devait encore faire l'objet d'une confirmation juridique est toujours compatible avec l'article 22 de la Constitution.

Le Comité permanent R a également formulé plusieurs observations spécifiques à propos du service Belgian Passenger Information Unit (BelPIU), cette unité

---

326 Le projet de loi a été déposé à la Chambre en février 2022, et adopté en Commission Intérieure – en deuxième lecture – le 3 mai 2022 (*Doc.Parl.* Chambre 2021-2022, 55-2443).

327 Cet arrêté royal a été pris en exécution de l'article 2, 1er alinéa, 2°, g), de la L.OCAM. Il désigne les services d'appui suivants : le service des Cultes et de la Laïcité de la Direction générale Législation, libertés et droits fondamentaux du SPF Justice, la Direction générale des Établissements pénitentiaires du SPF Justice, la Direction générale du Centre de crise du SPF Intérieur et l'Administration générale de la Trésorerie du SPF Finances.

placée par l'A.R. du 21 décembre 2017 sous la direction de la Direction générale Centre de crise du SPF lnterieur.[328]

Le Comité permanent R a souligné que le fait de placer le service BelPIU sous l'égide du Centre de crise n'a aucune influence sur le cadre juridique existant concernant le traitement des données des passagers par ce service. Malgré la désignation du Centre de crise comme service d'appui de l'OCAM, BELPIU ne peut être (indirectement) soumis aux modalités de coopération telles que décrites dans la L.OCAM.

S'il existe une nécessité de désigner le service BelPIU comme service d'appui de l'OCAM, il faut alors adapter la L.OCAM ainsi que la Loi du 25 decembre 2016 relative au traitement des données des passagers.

En outre, le croisement entre les informations de voyage détenues par BELPIU et les données de les BDC illustre la problématique plus large de la relation entre les activités de l'OCAM en sa qualité de gestionnaire opérationnel des BDC et l'OCAM en sa qualité d'organe d'évaluation de la menace, d'autre part (voir *infra*).

VI.6.2. MODIFICATION DES CONDITIONS DE NOMINATION DU DIRECTEUR ET DU DIRECTEUR ADJOINT

Le projet de loi visait aussi à supprimer l'une des conditions à remplir pour être designé directeur et directeur adjoint de l'OCAM, à savoir le statut requis de magistrat.

Le Comité permanent R indiquait dans son avis que cette suppression augmenterait certes le nombre de candidats possibles, mais posait un certain nombre de questions au regard de l'environnement légal complexe dans lequel l'OCAM évolue. La question se pose de savoir si la condition de nomination en remplacement d'une 'expertise juridique complémentaire' n'est pas plus théorique que réellement suffisante pour compenser la suppression du statut de magistrat au regard du respect d'un équilibre entre les besoins opérationnels de l'OCAM et l'importance du respect et de la connaissance des règles en vigueur. Le Comité permanent R constatait également que le projet de loi n'ajoutait aucune disposition pour protéger l'indépendance et l'impartialité de la direction de l'OCAM (tenant compte de la suppression proposée de la condition de nomination d'être un magistrat). Un tel cadre est toutefois nécessaire, notamment en ce qui concerne la réalisation d'évaluations de la menace et la définition du niveau de menace pertinent.

---

328 Article 2 de l'Arrêté royal relatif à l'exécution de la Loi du 25 decembre 2016 relative au traitement des données des passagers, reprenant diverses dispositions concernant l'Unité d'information des passagers et le délégué à la protection des données.

VI.6.3. EXTENSION DES MISSIONS DE L'OCAM

L'avant-projet de loi visait également à inscrire (à l'article 8 de la L.OCAM) des nouvelles missions pour l'OCAM.

VI.6.3.1. La coordination de l'approche globale des menaces

Le projet de loi prévoyait tout d'abord un rôle de coordination pour l'OCAM dans l'approche globale des menaces visées dans l'article 3 de la L.OCAM. L'exposé des motifs indiquait qu'il s'agissait de consolider une pratique déjà existante.

Les Comités permanents R et P constataient toutefois que le contenu de ce rôle de coordination n'était pas davantage precisé. L'exposé des motifs se limitait à une énumeration non exhaustive d'exemples tels que l'interaction entre les Local Task Force (LTF) et les Cellules de Securité lntegrale Locale en matière de radicalisme, d'extrémisme et de terrorisme (CSIL-R) et l'optimalisation des BDC. Les Comités recommandaient de préciser la mission de l'OCAM en matière de coordination de l'approche globale des menaces. En effet, l'OCAM ne dispose pas d'un arsenal opérationnel pour approcher les menaces de façon effective et globale.

Le Comité permanent R pointait en outre la définition excessivement vague et large de l'objet de la mission de coordination. Cela soulève d'abord la question des services qui relèveraient ou non de la coordination de l'OCAM. Se pose également la question de savoir quelle 'approche' doit etre coordonnée : s'agit-il de la coordination de l'approche globale du terrorisme, de l'extrémisme et de la radicalisation ou uniquement de la coordination de l'approche 'administrative' ? Cela concerne-t-il uniquement la coordination de l'approche 'strategique' ou également la coordination de l'approche 'opérationnelle' ? Enfin, se pose la question des instruments (contraignants ?) dont dispose l'OCAM pour concrétiser cette mission de coordination.

Le Comité permanent R constatait également que le projet créait une confusion entre plusieurs réglementations légales qui encadrent les missions de l'OCAM.[329] Le Comité indiquait qu'il conviendrait de clarifier la relation entre l'obligation d'alimenter les BDC dans le chef des 'services de base' et des 'services partenaires'[330] et l'obligation de notification à l'OCAM pour les 'services d'appui de l'OCAM'. En

---

329 En particulier, la L.OCAM, la réglementation autour des banques de données communes et la loi portant création des CSIL-R.

330 Les articles 44/2, § 2 et 44/11/3ter, § 4 LFP, *i.o.* article 7, § 1er de 'I' Arrete royal du 21 juillet 2016 AR Terrorist Fighters et article 7, § 1er AR Propagandistes de haine. Voir egalement la Circulaire du 22 mai 2018 du ministre de la Sécurité et de l'lntérieur et du ministre de la Justice 'relative à l'échange d'informations et au suivi des terrorist fighters et des propagandistes de haine' (Circulaire Terrorist fighters et Propagandistes de haine). Le Collège des procureurs fédéraux et le Ministère public ont eux aussi émis quelques circulaires en la matière : COL 10/2015 'concerne : Approche judiciaire en matière des foreign terrorist fighters', COL 21/2016 'concerne : Approche judiciaire des prédicateurs de haine' et COL 22/2016 'concerne : Banque de données commune relative aux Foreign Terrorist Fighters'.

effet, l'extension de l'obligation de notification à toutes les nouvelles missions de l'OCAM crée une ambiguité.

Le Comité permanent R invitait par ailleurs à clarifier si l'obligation de notification s'appliquait aux membres des CSIL-R également et, le cas échant, s'ils sont autorisés à fournir à l'OCAM des données à caractère personnel.

VI.6.3.2. De nouvelles missions confiées à l'OCAM par le Conseil national de sécurité ?

L'avant-projet de loi prévoyait ensuite que l'OCAM pouvait se voir attribuer, le cas échéant, de nouvelles missions dans la sphère de ses compétences par le Conseil national de sécurité au moyen d'un arrêté royal. Si l'extension de la liste des services d'appui par A.R. doit être confirmée dans une loi, une telle confirmation n'était pas exigée en ce qui concerne l'extension des missions de l'OCAM qui devait, selon l'avant-projet, uniquement faire l'objet d'un arrêté royal délibéré en Conseil des ministres. L'avis mettait en lumière cette différence d'approche instaurée au sein de la même loi.

Le Comité permanent R conseillait par ailleurs de clarifier davantage l'expression 'sphère de compétence de l'OCAM' dans la disposition concernée. En effet, il n'existe pas de sphère de compétence de l'OCAM qui soit uniforme pour toutes ses missions.[331]

Il était également proposé d'étendre l'obligation de notification des services d'appui à toutes les nouvelles missions de l'OCAM. Selon cette logique, les services d'appui seraient obligés de transmettre toutes les informations dont ils disposent à l'OCAM lorsque ces informations sont pertinentes pour des missions de l'OCAM fixées par arrêté royal. Cela inclut également les données à caractère personnel. Compte tenu du droit fondamental à la vie privée consacré par l'article 22 de la Constitution, l'avis rappelait que la transmissionet le traitement de données à caractère personnel doivent toujours être ancrés dans une loi formelle afin d'en fixer les règles et objectifs de base.

VI.6.4. COMMUNICATION ET CONSULTATION DES ÉVALUATIONS

L'avant-projet de loi visait également à modifier les conditions et modalités de communication, par l'OCAM, des évaluations stratégiques, ponctuelles ou effectuées à la demande d'un service d'appui. A ce propos, les Comités permanents

331 Ainsi, par exemple, la L.OCAM porte sur le terrorisme et l'extrémisme, y compris le processus de radicalisation tandis que la Loi sur la fonction de police (LFP) traite du terrorisme et de l'extrémisme pouvant mener au terrorisme.

P et R pointaient certaines incohérences (notamment linguistiques) dans le texte et suggèraient des formulations alternatives.

VI.6.5. COMMUNICATION ET CONSULTATION DE RENSEIGNEMENTS DE NATURE JUDICIAIRE SOUS EMBARGO[332]

L'avant-projet de loi visait aussi à modifier la L.OCAM en prévoyant notamment que les renseignements de nature judiciaire sous embargo ne soient plus uniquement transmis au directeur de l'OCAM mais également aux membres habilités de l'OCAM désignés pour réaliser l'évaluation *ad hoc* des renseignements sous embargo.

Les Comités permanents R et P conseillaient de prévoir expressément dans l'avant-projet de loi que la connaissance de ces renseignements sous embargo par les membres du personnel de l'OCAM désignés soit strictement indispensable pour l'exercice de leur fonction dans le cadre des missions de l'OCAM.[333] Les Comités recommandaient par ailleurs de reprendre expressément dans le texte de l'avant-projet de loi que le directeur de l'OCAM doit tenir la liste des membres du personnel désignés ayant accès à ces informations à la disposition des Comités permanents R et P.

VI.6.6. COMMUNICATION ET CONSULTATION DE RENSEIGNEMENTS VISÉS À L'ARTICLE 12, 1ER ALINÉA L.OCAM

L'avant-projet de loi prévoyait les mêmes adaptations en ce qui concerne les renseignements sous embargo fournis, par les services de renseignement et de securité, l'Administration des douanes et accises du SPF Finances et le SPF Affaires étrangères, provenant d'un service étranger homologue qui a explicitement demandé de ne pas les transmettre à d'autres services ou dont la transmission peut compromettre la securité d'une source humaine.

À l'instar de ce qui a été discuté *supra,* les Comités invitaient à reprendre expressément dans le texte que cet accès doit être déterminé selon le principe du besoin d'en connaitre et que le directeur de l'OCAM doit tenir la liste des membres du personnel designés ayant accès à ces informations à la disposition des Comités permanents R et P.

---

332 Voir egalement : COMITÉ PERMANENT R, *Rapport d'activites 2008*, 110.

333 Autrement dit, qu'ils aient strictement le besoin d'en connaitre.

CHAPITRE VII.
LES INFORMATIONS ET INSTRUCTIONS JUDICIAIRES

Le service d'Enquêtes R du Comité effectue également sur ordre des autorités judiciaires des enquêtes sur les membres des services de renseignement et de sécurité et de l'Organe de coordination pour l'analyse de la menace (OCAM)[334] suspectés d'avoir commis un crime et/ou un délit. Cette compétence est décrite à l'article 40, alinéa 3 de la L.Contrôle.

Lorsqu'ils remplissent une mission de police judiciaire, les membres et le directeur du service d'Enquêtes R sont soumis à l'autorité du procureur général près la cour d'appel ou du procureur fédéral (art. 39 L.Contrôle). Le Comité permanent R n'a aucune autorité sur eux. Le président du Comité doit cependant veiller à ce que l'exécution des missions de police judiciaire n'entrave pas l'exécution des enquêtes de contrôle. La raison en est évidente : le Comité a beaucoup d'autres missions légales. Celles-ci pourraient être mises en péril si les dossiers judiciaires nécessitaient un investissement trop conséquent. Le président peut, le cas échéant, se concerter avec les autorités judiciaires quant à la participation des membres du service d'Enquêtes R à des enquêtes pénales (art. 61*bis* L.Contrôle).

Lorsque le service d'Enquêtes R effectue des enquêtes pénales, le directeur doit remettre un rapport au Comité permanent R au terme de celles-ci. Dans ce cas, '*le rapport se limite aux informations qui sont nécessaires à l'accomplissement par le Comité permanent R de ses missions*' (art. 43, alinéa 3, L.Contrôle).

En 2021 le service d'Enquêtes R a effectué des devoirs d'enquête dans le cadre de six dossiers répressifs ; quatre sous l'autorité du Parquet fédéral, un à l'Auditorat du travail de Liège et un auprès du Procureur du Roi de Bruxelles. Cinq de ces dossiers concernaient potentiellement des membres du Service Général du Renseignement et de la Sécurité et un dossier des membres de la Sûreté de l'État. Dans ce cadre, le service d'Enquêtes R a reçu six apostilles et en a clôturées quatre.

Au total, dix procès-verbaux ont été dressés et onze rapports confidentiels ont été rédigés. Les infractions suivantes étaient visées dans le cadre de ces dossiers : 'violation du secret professionnel', 'faux et usage de faux en écriture' et 'consultation irrégulière de bases de données'.

---

[334] En ce qui concerne les membres des autres 'services d'appui' de l'OCAM, cette disposition ne s'applique qu'à l'égard de l'obligation de communiquer des renseignements pertinents à l'OCAM (articles 6 et 14 L.OCAM).

Par ailleurs, l'article 50 L. Contrôle dispose que *'[t]out membre d'un service de police qui constate un crime ou un délit commis par un membre d'un service de renseignement rédige un rapport d'information et le communique dans les quinze jours au chef du Service d'enquêtes R*'. En 2021, le service d'Enquêtes R n'a reçu aucun signalement en ce sens.

CHAPITRE VIII.
EXPERTISE ET CONTACTS EXTERNES

VIII.1. EXPERT DANS DIFFÉRENTS FORUMS

En 2021, les membres du Comité permanent R et son personnel ont été consultés à plusieurs reprises en tant qu'experts par des institutions publiques et privées nationales et étrangères:

- Le greffier faisant fonction du Comité permanent R a été invité, dans le cadre du cours « Intelligence » du Master en relations internationales et diplomatie (Université d'Anvers), à présenter le fonctionnement du Comité. L'intervention s'est déroulée par vidéoconférence ;
- Des articles rédigés par des collaborateurs du Comité ont été publiés dans diverses revues scientifiques[335] ;
- Le président a été invité, en mai 2021, à faire partie du comité de sélection pour la nomination d'un membre suppléant pour la Commission BIM. L'objectif de cette sélection et du comité de sélection était de recueillir des informations utiles sur les candidats afin de pouvoir donner un avis motivé au ministre de la Justice ;
- En juin 2021, le président est intervenu, à la demande de la Rapporteuse spéciale sur les droits de l'homme et la lutte antiterrorisme, en tant que modérateur à *RightsCon*, conférence mondiale sur les droits de l'homme à l'ère numérique. La conférence, organisée en collaboration avec l'Agence AWO, avait pour thème '*When States of Emergency Collide : COVID-19, Counter-Terrorismmand Transnational Data Flows*' ;
- Plusieurs vidéoconférences ont eu lieu entre des juristes du Comité permanent R et des représentants de l'Institut fédéral pour la protection et la promotion des droits humains (*infra*) au sujet de l'obligation de notification active suite à la mise en œuvre de méthodes particulières de recueil de données.

---

335 F. GIVRON et S. LIPSZYC, 'Le contentieux en matière de sécurité et son instance spécifique: l'Organe de recours en matière d'habilitations, attestations et avis de sécurité. La recherche de l'équilibre entre la protection des droits de la défense et la préservation des intérêts majeurs de l'État', *J.T.*, 2021/3, 45-53; W. VAN LAETHEM, 'Problemen met veiligheidsadvies van beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen', *Juristenkrant*, 2021, 439, 8-9 ; B. VERSCHAEVE, 'Het Incident Respons Team van de Staatveiligheid. De interne beveiligingsdienst van de burgerlijke inlichtingendienst toegelicht', *Politie en Recht*, 1, 2022, 3-20.

- Des échanges ont eu lieu avec des personnes issues du monde académique (Université d'Anvers) sur la place croissante qu'occupent les informations issues des services de renseignement dans la motivation (de tout type) de décision(s) administrative(s) ;
- En septembre 2021, le greffier faisant fonction a été invité à faire une présentation sur le cadre théorique des screenings de sécurité en Belgique lors d'une journée d'étude organisée à huis clos. Elle s'adressait aux chercheurs ainsi qu'aux personnes issues du monde du renseignement et des infrastructures critiques. L'ensemble de l'événement s'inscrivait dans le cadre d'une thèse de doctorat sur l''*insider threat*' (Université d'Anvers) ;
- Toujours en septembre, à la demande du ministre du gouvernement de la Fédération Wallonie-Bruxelles compétent pour les Maisons de justice, le Comité a participé à une réunion sur l'échange d'informations entre les Maisons de justice, l'Organe de coordination pour l'analyse de la menace (OCAM) et la Sûreté de l'État (VSSE) ;
- Le Directeur du service d'Enquêtes a participé à une session de formation pour les personnes nouvellement recrutées au sein du Service Général du Renseignement et de la Sécurité (SGRS).
- En octobre 2021, le président du Comité permanent R a pris la parole lors de la troisième 'European Intelligence Oversight Conference ' organisée à Rome.[336]
- Un collaborateur a finalisé sa thèse de doctorat et obtenu le titre de Docteure en Sciences politiques et sociales en décembre 2021 (UCLouvain Saint Louis Bruxelles).[337]

VIII.2. PROTOCOLE DE COOPÉRATION AVEC LES MÉDIATEURS FÉDÉRAUX

La Loi du 15 septembre 2013[338] désigne les Médiateurs fédéraux[339] comme point de contact central des atteintes suspectées à l'intégrité au sein des autorités administratives fédérales. En septembre 2021, le 'Protocole de coopération du 7 octobre 2021 pour les relations entre les Médiateurs fédéraux et le Comité permanent de contrôle des services de renseignement et de sécurité dans le cadre de la loi du 15 septembre 2013' a été conclu. Le protocole vise à réglementer les modalités de coopération entre les Médiateurs fédéraux et le Comité lorsqu'une

336 Le titre de son intervention était : '*European case law on the notification of secret measures and the Belgian response with particular attention to the future rol of the Standing Committee R*'.

337 C. THOMAS, "*Une menace possible et vraisemblable*" *Dire et faire la sécurité : l'Organe de coordination pour l'analyse de la menace et la structuration du champ antiterroriste belge*, Bruxelles, UCLouvain Saint Louis Bruxelles, septembre 2021, 470p.

338 Loi du 15 septembre 2013 relative à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel, *M.B.* 14 octobre 2013.

339 Loi du 22 mars 1995 instaurant des médiateurs fédéraux, *M.B.* 7 avril 1995.

une atteinte suspectée à l'intégrité dans l'un des deux services de renseignement est signalée aux Médiateurs.

Le cas échéant, les Médiateurs fédéraux peuvent demander au Comité permanent R de désigner un membre du service d'Enquêtes pour assister le Centre Intégrité – un point de contact central au sein des Médiateurs fédéraux – en tant qu'expert dans la conduite de l'enquête. Des accords ont également été conclus dans le protocole concernant les moyens d'investigation, le secret professionnel, la confidentialité et l'échange de bonnes pratiques.

VIII.3. COLLABORATION AVEC L'INSTITUT FÉDÉRAL DES 'DROITS DE L'HOMME'

Avec la Loi du 12 mai 2019, l'Institut fédéral pour la protection et la promotion des droits humains (IFDH) a été créé.[340] Par le biais d'un protocole de coopération, toutes les institutions participantes ont accepté d'échanger des pratiques et des méthodes, d'examiner des questions communes et de promouvoir la coopération mutuelle. La contribution des partenaires a été sollicitée pour la rédaction d'un premier plan stratégique. Il a également été demandé au Comité un échange de vues avec les représentants de l'IFDH dans le cadre de la réalisation d'un rapport alternatif pour le Comité contre la Torture (CAT) de l'ONU. Cela concernait notamment les 'restitutions extraordinaires'[341], et relevait donc du mandat du Comité permanent R.

VIII.4. UNE INITIATIVE MULTINATIONALE EN MATIÈRE D'ÉCHANGE D'INFORMATIONS

La multiplication des échanges de données au niveau international entre les services de renseignement et de sécurité pose un certain nombre de défis aux organes de contrôle nationaux. Les organes de contrôle de (au départ) cinq pays européens (la Belgique, le Danemark, les Pays-Bas, la Norvège et la Suisse) se concertent depuis quelques années afin de relever ces défis, en identifiant des méthodes de travail qui leur permettraient de limiter le risque de lacunes dans le contrôle. Un nouveau partenaire a été impliqué ultérieurement dans ce projet, à savoir l'*Investigatory Powers Commissioner's Office (IPCO)* du Royaume-Uni. Le groupe a été rebaptisé '*Intelligence Oversight Working Group*' (IOWG) et, en 2019, a été élargi à trois observateurs, à savoir le *Swedisch Foreign Intelligence Inspectorate*

340 Loi du 12 mai 2019 portant création d'un Institut fédéral pour la protection et la promotion des droits humains, *M.B.* 21 juin 2019.

341 Voir *in extenso*, COMITÉ PERMANENT R, *Rapport d'activités 2006*, 34-41, ('II.2. Les vols CIA').

(Statens inspektion av försvarunderättelse-verksamhet (SIUN)), le *Swedish Board of Inventions (Statens uppfinnarnämnd, (SUN))* et la Commission G10 allemande.

En raison des restrictions liées à la crise sanitaire, les activités internationales sont restées limitées en 2021. En septembre 2021, une réunion virtuelle organisée par l'autorité de surveillance suisse *Autorité de surveillance indépendante des activités de renseignement* (AS-Rens) a eu lieu pour échanger sur l'avenir de l'IOWG. Les discussions ont également porté sur la manière dont les organes de contrôle font face à la pandémie et aux nouveaux développements technologiques dans le domaine du renseignement. Cette coopération sera intensifiée en 2022.

VIII.5. CONTACTS AVEC DES ORGANES DE CONTRÔLE ÉTRANGERS

En octobre 2021 s'est tenue la troisième conférence *European Intelligence Oversight Conference* auprès de l'organe de contrôle italien, la *Procura Generale della Corte di Cassazione*. La conférence a abordé des thèmes tels que '*The developments in the light of European Case Law*', '*Bulk data collection and targeted interceptions*' et '*International cooperation and other oversight developments in the light of the revised Convention 108+*'.

Dans le prolongement d'un questionnaire sur l'"*ex ante oversight*', l'organe de contrôle néerlandais CTIVD (*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten)* a lancé, en juillet 2020, une initiative similaire. Il s'agissait d'un questionnaire portant sur le '*complaint handling*' (traitement des plaintes). L'objectif de cette initiative était de recueillir et analyser les meilleures pratiques en Europe en matière de traitement des plaintes à des fins d'amélioration. Le Comité y a apporté sa contribution.

Le Comité permanent R a expliqué son intention de procéder, avec *l'Autorité de surveillance indépendante des activités de renseignement* (AS-Rens) suisse, à un échange de personnel dans le cadre d'un stage, même de courte durée. Après une suspension du projet en raison de la crise sanitaire, cet échange est prévu dans le courant de l'année 2022.

Le *Danish Intelligence Oversight Board* a partagé avec les organes de contrôle belge et européens ses '*Standards for Danish intelligence oversight activities*'.

Enfin, des informations ont été échangées avec la Cour administrative du Luxembourg concernant la législation relative à l'utilisation de documents classifiés dans le cadre des habilitations de sécurité.

CHAPITRE IX.
L'ORGANE DE RECOURS EN MATIÈRE D'HABILITATIONS, D'ATTESTATIONS ET D'AVIS DE SÉCURITÉ[342]

Ce chapitre reprend le rapport d'activités approuvé lors de la réunion du 20 mai 2022 par l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité (ci-après l'Organe de recours) ainsi qu'un certain nombre de remarques et suggestions du président de cette juridiction.

IX.1. LE RAPPORT D'ACTIVITÉS DE L'ORGANE DE RECOURS

IX.1.1. INTRODUCTION

L'Organe de recours[343] est, en Belgique, l'unique juridiction administrative compétente pour les contentieux portant sur des décisions administratives dans divers domaines : les habilitations de sécurité, les attestations de sécurité et, enfin, les avis de sécurité.

L'Organe de recours intervient également en tant que 'juge d'annulation' contre des décisions d'autorités publiques ou administratives, lorsqu'elles imposent des avis ou des attestations de sécurité pour un secteur, un lieu ou un événement donné.[344]

L'Organe de recours est composé du président du Comité permanent R, de la présidente du Comité permanent P et du président de la Chambre contentieuse de l'Autorité de protection des données. Les trois présidents peuvent être remplacés

---

342 Le présent rapport d'activités exécute l'article 13 de la Loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité qui stipule que l'organe de recours est tenu de rédiger un rapport annuel.

343 GIVRON, F. et LIPSZYC, S., 'Le contentieux en matière de sécurité et son instance spécifique : l'Organe de recours en matière d'habilitations, attestations et avis de sécurité. La recherche de l'équilibre entre la protection des droits de la défense et la préservation des intérêts majeurs de l'État', *J.T.*, 2021/3, 45-53.

344 Pour plus de détails, voir COMITÉ PERMANENT R, *Rapport d'activités 2006*, 87-120 et *Rapport d'activités 2018*, 111-124.

en cas d'empêchement par un membre-conseiller effectif de l'institution à laquelle appartient le président concerné.

Le président du Comité permanent R assure la présidence de l'Organe de recours. La fonction de greffier est exercée par le greffier du Comité permanent R et le personnel du greffe est le personnel affecté par le Comité. Les activités de l'Organe de recours constituent depuis plus de vingt ans l'exemple parfait de synergie au sein de certaines institutions satellitaires du Parlement. La composition de l'Organe de recours apporte en outre une contribution multidisciplinaire à la délibération de chaque dossier.

Il convient de noter qu'en ce qui concerne les recours, l'administration et le suivi sont entièrement assurés par le Comité permanent R. En effet, le Comité met à disposition toutes les personnes et ressources nécessaires pour assurer l'administration, la correspondance, la tenue des audiences et la rédaction des décisions. Il s'agit, d'une part, de la mise à disposition du président et de ses membres suppléants, de son greffier mais aussi des juristes comme '*greffiers assumés*' et du personnel administratif qui forment le greffe de cette juridiction administrative. D'autre part, le Comité permanent R prend en charge, sur son budget, les frais de locaux et de fonctionnement de l'Organe de recours.

L'Organe de recours a pris toutes les mesures nécessaires pour assurer son fonctionnement nonobstant la pandémie du COVID-19. L'Organe de recours a ainsi maintenu ses audiences au rythme minimum de deux par mois. En 2021, il a tenu 30 audiences.[345]

IX.1.2. LE DÉTAIL DES CHIFFRES

Cette section reprend les chiffres relatifs à la nature des décisions contestées, la qualité des autorités compétentes et des requérants, ainsi que la nature des décisions de l'Organe de recours dans le cadre des différentes procédures de recours. À des fins de comparaison, les chiffres des cinq années précédentes sont également repris.

En 2021, 180 recours ont été introduits, contre 144 en 2020 et 196 en 2019 (*infra*). On constate que ces chiffres suivent la reprise économique et la demande d'avis de sécurité notamment dans le secteur aéroportuaire et pour les candidats à la Défense.

149 décisions finales ont été prises.

345 Dont 13 audiences en néerlandais et 17 en français.

Tableau 1. Nombre de recours introduits (2016-2021)

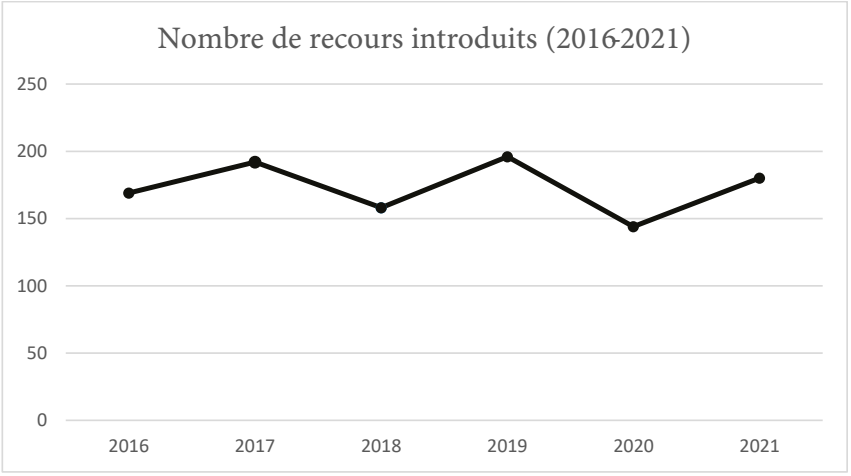


Tableau 2. Nombre de recours introduits *vs* nombre de décisions rendues (2016-2021)

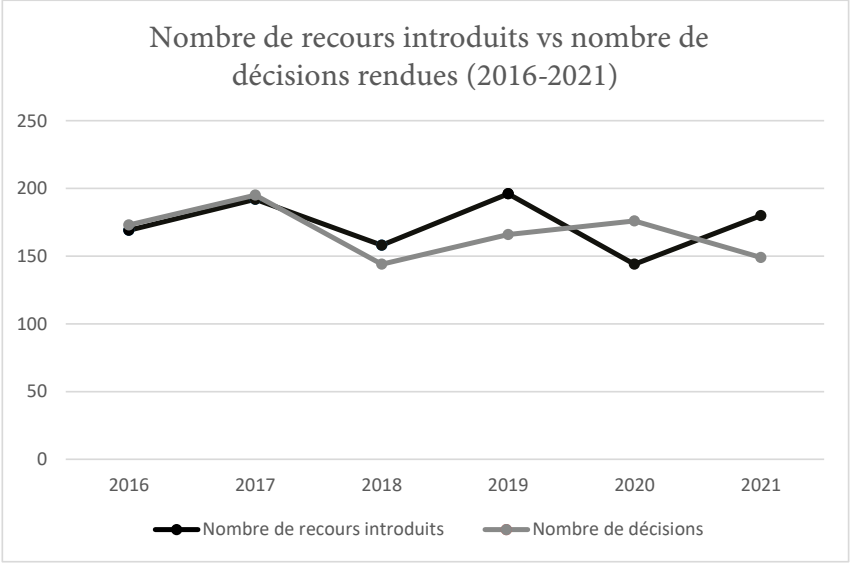


Tableau 3. Autorités de sécurité concernées (2016-2021)

	2016	2017	2018	2019	2020	2021
Autorité nationale de sécurité	92	129	113	114	91	86
Sûreté de l'État	0	0	0	0	0	4
Service Général du Renseignement et de la Sécurité	68	53	32	61	41	84
Agence fédérale de Contrôle nucléaire	8	7	10	17	7	6
Police fédérale	1	3	3	3	4	0
Police locale	0	0	0	1	1	0
TOTAL	**169**	**192**	**158**	**196**	**144**	**180**

Le graphique ci-dessous visualise la répartition des autorités de sécurité concernées en 2021.

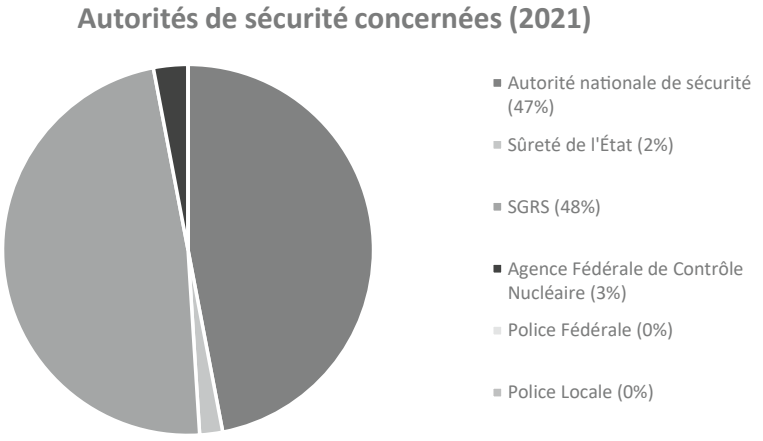


Tableau 4. Nature des décisions contestées

	2016	2017	2018	2019	2020	2021
Habilitations de sécurité (art. 12 et s. L.C&HS)						
Confidentiel	5	1	2	5	0	2
Secret	38	33	31	39	27	50
Très secret	7	6	3	7	5	8
Refus	28	30	26	39	23	37

	2016	2017	2018	2019	2020	2021
Retrait	9	7	4	16	8	17
Refus et retrait	0	0	0	0	0	4
Habilitation pour une durée limitée	4	1	1	3	0	1
Habilitation pour un niveau inférieur	1	0	0	0	0	
Pas de décision dans les délais	7	2	5	0	0	1
Pas de décision dans les nouveaux délais	1	0	0	0	0	0
Autres					1[346]	
SOUS-TOTAL HABILITATIONS DE SÉCURITÉ	50	40	36	51	32	60
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)						
Refus	1	3	3	1	0	3
Retrait	0	0	0	0	0	0
Pas de décision dans les délais	0	0	0	0	0	
Attestations de sécurité lieu ou événement (art. 22*bis*, al.2 L.C&HS)						
Refus	9	20	15	12	6	2
Retrait	0	0	0	0	0	0
Pas de décision dans le délai	0	0	0	0	0	1
Attestations de sécurité lieu secteur nucléaire (art. 8*bis* L.C&HS)						
Refus	7	7	11	17	7	6
Retrait	1	0	0	0	0	0
Pas de décision dans le délai	0	0	1	0	0	0
Avis de sécurité (art. 22*quinquies* L.C&HS)						
Avis négatif	101	122	92	115	99	108
Pas d'avis	0	0	0	0	0	0
Révocation d'avis positif	0	0	0	0	0	0
Actes normatifs d'une autorité administrative (art. 12 L. Org.recours)						

346 'Mise en garde du requérant'. Une personne s'était vue octroyer l'habilitation de sécurité pour cinq ans avec une mise en garde. Il est allé en recours contre cette mise en garde.

	2016	2017	2018	2019	2020	2021
Décision d'une autorité publique d'exiger des attestations de sécurité	0	0	0	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des attestations de sécurité	0	0	0	0	0	0
Décision d'une autorité administrative d'exiger des avis de sécurité	0	0	0	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des avis de sécurité	0	0	0	0	0	0
SOUS-TOTAL ATTESTATIONS ET AVIS	119	152	122	145	112	120
TOTAL DÉCISIONS CONTESTÉES	**169**	**192**	**158**	**196**	**144**	**180**

Tableau 5. Nature du requérant

	2016	2017	2018	2019	2020	2021
Fonctionnaire	2	4	5	4	8	16
(candidat) Militaire	23	20	8	27	39	81
Particulier	139	164	140	163	95	80
Personne morale	5	4	5	2	2	3

Le graphique ci-dessous visualise la répartition 'nature du requérant' en 2021.

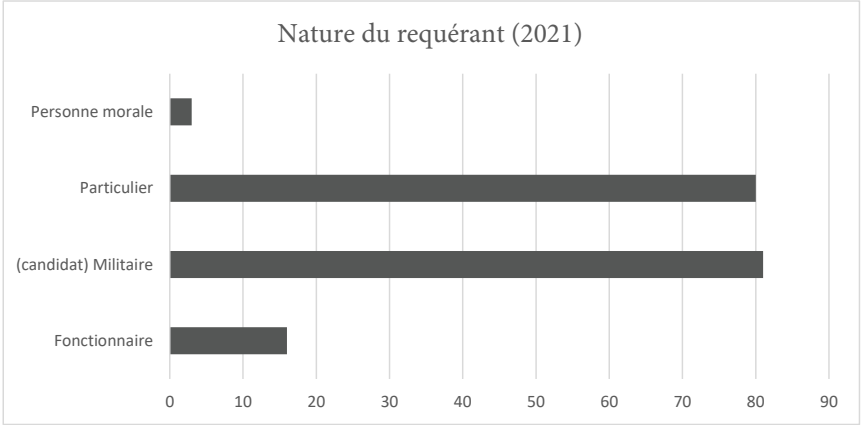


Tableau 6. Langue du requérant

	2016	2017	2018	2019	2020	2021
Français	99	115	83	101	83	86 (1)
Néerlandais	70	77	75	95	61	94 (2)
Allemand	0	0	0	0	0	0
Autre langue	0	0	0	0	0	0

(1) 86 dossiers francophones en 2021 + 29 dossiers francophones des années antérieures mais traités en 2021 = 115 requérants francophones

(2) 94 dossiers néerlandophones en 2021 + 18 dossiers néerlandophones des années antérieures mais traités en 2021 = 112 requérants néerlandophones

Tableau 7. Actes du greffe

	2016	2017	2018	2019	2020	2021
Demande du dossier complet (1)	167	191	154	191	141	180
Demande d'informations complémentaires (2) et rappels adressés aux autorités de sécurité (3)*	23	36	12	39	41	45

(1) L'Organe de recours peut demander l'intégralité du dossier aux autorités de sécurité. Comme ce dossier contient davantage de données que le rapport d'enquête seul, cette requête est systématiquement effectuée par le greffe.

(2) L'Organe de recours peut également demander tout complément d'informations qu'il juge nécessaire pendant la procédure. Dans la pratique, le greffe se charge de demander aux autorités de compléter les dossiers.

(3) L'art. 6 de l'AR Org. recours prévoit les délais pour la communication des dossiers par les autorités de sécurité. Ces délais prennent cours lorsque le greffier transmet une copie du recours à l'autorité de sécurité concernée. Ils varient selon la nature de l'acte attaqué. Ainsi, l'autorité de sécurité doit communiquer son dossier dans les 15 jours en ce qui concerne les habilitations de sécurité, dans les 5 jours en matière d'attestations de sécurité et dans les 10 jours si le recours porte sur un avis de sécurité. Lorsque ces délais ne sont pas respectés, le greffe prend les contacts nécessaires. Ces données sont comptabilisées à partir de 2019.

Tableau 8. Actes juridictionnels interlocutoires pris par l'Organe de recours [347]

	2016	2017	2018	2019	2020	2021
Audition d'un membre d'une autorité (1)	10	0	1	6	1	4
Décision du président (2)	0	0	0	0	0	0
Soustraction d'informations du dossier par l'Organe de recours (3)	54	80	72	77	50	77
Décisions avant dire droit (4)	/	/	/	9	9	19

(1) L'Organe de recours peut décider d'entendre les membres des services de renseignement et de police ou des autorités de sécurité qui ont participé à l'enquête ou à la vérification de sécurité.

(2) Le président de l'Organe de recours peut décider de permettre au membre du service de renseignement de garder secrètes certaines données pendant son audition.

(3) Si le service de renseignement ou de police concerné le demande, l'Organe de recours peut décider que certaines informations soient retirées du dossier communiqué au requérant.

(4) Il peut s'agir par exemples d'une décision de jonction de deux dossiers ou de demander un complément d'informations à propos de la situation d'un dossier judiciaire. Ces données sont comptabilisées à partir de 2019.

Tableau 9. Manière dont le requérant fait usage de ses droits de défense

	2016	2017	2018	2019	2020	2021
Consultation du dossier par le requérant et/ou l'avocat	87	105	69	96	96	97
Audition du requérant (assisté ou non d'un avocat)[348]	127	158	111	143	135	151

347 Le nombre d'"actes juridictionnels interlocutoires' (tableau 6), les 'manières dont les requérants font usage de leurs droits de défense' (tableau 7), ou encore la 'nature des décisions de l'Organe de recours' (tableau 8) ne correspondent pas nécessairement au nombre de requêtes introduites (voir tableaux 1 à 4). En effet, certains dossiers ont par exemple déjà été ouverts en 2020, alors que la décision n'a été rendue qu'en 2021.

348 La L.Org.recours prévoit l'assistance d'un avocat à l'audience mais pas la représentation par ce dernier. À noter que, dans le cadre de certains dossiers, le requérant (assisté ou non de son avocat) est auditionné à plusieurs reprises.

Tableau 10. Nature des décisions de l'Organe de recours

	2016	2017	2018	2019	2020	2021
Habilitations de sécurité (art. 12 et s. L.C&HS)						
Recours irrecevable	0	3	0	1	1	0
Recours sans objet	7	0	4	3	3	3
Recours non fondé	18	13	12	12	16	11
Recours fondé (avec octroi partiel ou complet)	24	24	12	25	14	17
Devoir d'enquête complémentaire par l'autorité	2	0	1	1	2	1
Délai supplémentaire pour l'autorité	2	1	1	0	3	0
Donne acte de retrait de recours	0	0	3	2	2	11
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)						
Recours irrecevable	0	1	0	0	0	0
Recours sans objet	0	1	0	0	0	0
Recours non fondé	1	0	1	1	0	2
Recours fondé (avec octroi)	1	1	0	3	0	2
Donne acte de retrait de recours	-	-	-	1	0	0
Attestations de sécurité pour lieux ou événements (art. 22*bis*, al.2 L.C&HS)						
Recours irrecevable	0	1	2	4	2	0
Recours sans objet	0	1	0	0	0	0
Recours non fondé	2	12	2	4	4	1
Recours fondé (avec octroi)	4	7	3	4	1	0
Donne acte de retrait de recours	0	1	2	0	0	0
Attestations de sécurité pour le secteur nucléaire (art. 8*bis* §2 L.C&HS)						
Recours irrecevable	1	1	0	1	0	0
Recours sans objet	1	0	1	0	0	0
Recours non fondé	0	1	1	5	2	2
Recours fondé (avec octroi)	7	5	6	7	4	6
Donne acte de retrait de recours	-	-	2	0	0	0

	2016	2017	2018	2019	2020	2021
Avis de sécurité (art. 22*quinquies* L.C&HS)						
Organe de recours non compétent	0	20[349]	12	0	0	0
Recours irrecevable	15	10	3	7	8	3
Recours sans objet	0	1	3	1	6	4
Confirmation de l'avis négatif	42	49	46	40	51	47
Réformation en avis positif	46	41	27	43	52	34
Donne acte de retrait de recours	0	1	0	1	5	5
Recours contre des actes normatifs d'une autorité administrative (art. 12 L. Org.recours)	0	0	0	0	0	0
TOTAL	**173**	**195**	**144**	**166**	**176**	**149**

IX.2. REMARQUES ET SUGGESTIONS DU PRÉSIDENT DE L'ORGANE DE RECOURS

IX.2.1. UNE PROCÉDURE PARTICULIÈRE ET COMPLEXE

La juridiction administrative qu'est l'Organe de recours se caractérise par une gestion administrative des dossiers particulière et plus complexe par rapport aux autres juridictions de l'ordre judiciaire et administratif.

Une première particularité est l'exigence légale de l'article 4 de la Loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité (L.Org.recours) qui paraît aujourd'hui démesurée. En effet, le justiciable doit former son recours en matière d'attestations et d'avis de sécurité dans le délai strict de huit jours, par lettre recommandée. Il est indéniable pour les praticiens qu'un tel délai est résolument trop court pour le citoyen.

Une seconde particularité est que le requérant doit, au regard de la loi, faire un exposé dans son recours des circonstances de la cause et des raisons invoquées. Le président de l'Organe de recours est conscient que le prescrit légal ne prend pas en compte la difficulté du citoyen à ester en justice.

---

[349] Il s'agissait en l'espèce de recours introduits contre des avis de sécurité (négatifs) rendus par l'Autorité nationale de sécurité concernant le personnel de sous-traitants actifs pour les institutions européennes. L'Organe de recours avait décidé que les avis formulés par l'Autorité nationale de sécurité n'avaient pas de base juridique. En conséquence, l'Organe de recours s'était déclaré sans compétence pour statuer sur le bien-fondé ou non des avis de sécurité rendus par l'Autorité nationale de sécurité.

Une troisième particularité est liée à la demande des autorités de sécurité, dans près d'un dossier sur deux (77/180), de restriction du droit du justiciable à prendre connaissance de l'intégralité de son dossier. Il est, en effet, demandé à l'Organe de recours de faire application de l'article 5 §3 L.Org.recours. Pour rappel, cet article stipule que « *A la demande d'un service de police ou de renseignement, l'organe de recours peut décider que certaines informations figurant dans la déposition d'un membre d'un service de police ou de renseignement visé au § 2, dans le rapport d'enquête ou dans le dossier d'enquête ou de vérification sont secrètes pour un des motifs visés au § 2, alinéa 4, ou parce qu'elles relèvent du secret d'une information ou d'une instruction judiciaire en cours, et qu'elles ne pourront être consultées ni par le requérant ni par son avocat. Si ces secrets concernent une information ou une instruction judiciaire en cours, l'organe de recours se concerte au préalable à ce sujet avec le magistrat compétent. Lorsque ces informations proviennent d'un service de renseignement étranger, la décision de non-consultation est prise par le service de renseignement et de sécurité. Ces décisions ne sont susceptibles d'aucun recours*.» Il en résulte que la préparation des dossiers de l'Organe de recours nécessite que ceux-ci soient scannés puis 'caviardés'. Ce travail se réalise page par page, paragraphe par paragraphe ou mots par mots par le greffe. *In concreto*, il s'agit d'une analyse juridique, approuvée par le président de la juridiction et mise en œuvre par les membres du greffe. Il s'agit pour la juridiction de garantir le droit du justiciable à être mis en possession d'un maximum d'informations face à une demande légale de restriction d'accès.

Une quatrième particularité est due au délai de transmission des dossiers administratifs par les autorités de sécurité et cela nonobstant le prescrit légal. Le greffe de l'Organe de recours a dû adresser dans 45 des 180 dossiers introduits, un ou plusieurs rappels aux autorités de sécurité pour obtenir le dossier administratif. Ces retards se sont multipliés et touchent un dossier sur quatre contre un dossier sur dix il y a encore cinq ans. Par conséquent, l'Organe de recours ne peut pas rendre ses décisions dans les délais impartis. Au-delà, il en résulte avant tout un préjudice pour le justiciable pour qui l'obtention de l'habilitation ou de l'avis de sécurité est le plus souvent la condition *sine qua non* à l'exercice d'une fonction.

Enfin, une cinquième particularité consiste en la multiplication des recours déposés par des demandeurs étrangers ou ayant séjourné à l'étranger et l'inadéquation des outils légaux à disposition des autorités de sécurité pour répondre à cette réalité sociale. Il en résulte parfois la nécessité pour les autorités de sécurité de conclure des traités permettant l'échange d'informations et de renseignements avec des autorités de sécurité étrangères. En l'absence de tels accords, les autorités de sécurité, sans motivation circonstanciée, ne suivent pas la jurisprudence de l'Organe de recours en ce qui concerne la problématique des enquêtes ou des vérifications sur des personnes qui n'ont pas la nationalité belge. Le président de l'Organe de recours considère que les autorités de sécurité belges

devraient chercher à obtenir des informations auprès des services homologues étrangers.[350]

Pour le président de l'Organe de recours, la loi et ses arrêtés royaux ne sont plus en phase avec les exigences modernes d'accès à la justice. En effet, les articles 2 et 3 de l'AR Org. recours, stipulent respectivement que *'l'envoi à l'organe de recours de toutes pièces de procédure se fait sous pli recommandé à la poste'* et que *'le recours est signé et daté par le requérant ou par son avocat'*. De nombreux justiciables ne respectent pas ces règles, le plus souvent en raison d'une maîtrise imparfaite (mais compréhensible au vu de leur complexité) des règles de procédure.

C'est le sens de la proposition de loi rédigée, par le président de l'Organe de recours avec l'aide, comme expert, de l'ancien président de la Cour de cassation, Ivan Verougstraete. Il y a lieu, en effet, de mieux prendre en compte la qualité, voire la fragilité, de nombreux requérants et de prévoir des dispositions légales qui n'entraînent pas la nullité de plein droit ou l'irrecevabilité de la requête.

On relèvera que le texte de réforme a été adressé à la Chambre des représentants le 24 novembre 2020. Compte tenu des différentes propositions de loi en préparation modifiant entre autres la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (L.C&HS), l'Organe de recours estime qu'il convient d'établir un lien avec ce texte de réforme. Après tout, la règlementation concernant les habilitations, attestations et avis de sécurité doit être reliée de manière harmonieuse aux règlements concernant le recours éventuel contre ces décisions administratives.

Le 14 février 2022, la présidente de la Chambre a, en réponse, adressé un courrier au président de la juridiction administrative en insistant notamment sur une nouvelle concertation avec le Comité permanent P et la Chambre contentieuse de l'Autorité de Protection des données.

L'accessibilité à la juridiction administrative reste la priorité de l'Organe de recours. Le texte tel que rédigé avait pour but de consacrer l'Organe de recours comme juge naturel des questions de sécurité, d'harmoniser les délais de recours, de faciliter la procédure et de rendre sa digitalisation possible.

IX.2.2. DÉCISION DU CONSEIL D'ÉTAT

Dans un cas particulier, le requérant s'est pourvu 'en cassation' devant le Conseil d'État contre une décision de l'Organe de recours. C'était la première fois depuis

[350] Par la loi du 23 février 2018 (*M.B.* 1er juin 2018), le législateur a explicitement donné à la police et aux services de renseignement le pouvoir de solliciter des informations pertinentes auprès des services partenaires étrangers dans le cadre d'une vérification de sécurité (voir article 22*sexies*, 3° L. C&HS et *Doc. parl.* Chambre, 2017-2018, 54 2767/001, 13). Par cette disposition, le législateur a décidé que, outre le fait qu'une vérification de sécurité ne se limite pas toujours à une simple vérification de certaines bases de données, des informations étrangères peuvent être pertinentes pour une vérification de sécurité.

la création de l'Organe de recours en 1998. Le Conseil d'État a pourtant déclaré le recours recevable[351], bien que non fondé.[352]

IX.2.3. RESPONSABILITÉ DE L'ORGANE DE RECOURS

Nonobstant l'absence de personnalité juridique dans le chef de l'Organe de recours, à la suite d'une décision de la juridiction administrative et d'un arrêt d'incompétence du Conseil d'État, un justiciable a lancé une action en responsabilité. Citation fut introduite devant le Tribunal francophone de Première instance de Bruxelles. Relevons qu'il avait non seulement cité l'État belge, mais également l'Organe de recours. Cette affaire est pendante devant la Cour d'appel de Bruxelles à la suite du jugement rendu le 7 septembre 2018 par la juridiction d'instance mentionnée qui avait condamné l'Organe de recours au paiement d'un dommage.

IX.2.4. DEUX QUESTIONS AU REGARD DE L'ARTICLE 6 DE LA CONVENTION EUROPÉENNE DES DROITS DE L'HOMME (CEDH)

Le président de l'Organe de recours estime approprié de sensibiliser la Chambre des représentants sur les questions soulevées par la jurisprudence européenne et que la Loi organique sur l'Organe de recours n'a pas, jusqu'à ce jour, envisagées.

En effet, l'article 6 de la CEDH consacre le droit à un procès équitable tant en matière judiciaire qu'administrative. Il vise en son alinéa premier notamment la question de la publicité des audiences et du prononcé des décisions à intervenir :
"Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle. Le jugement doit être rendu publiquement, mais l'accès de la salle d'audience peut être interdit à la presse et au public pendant la totalité ou une partie du procès dans l'intérêt de la moralité, de l'ordre public ou de la sécurité nationale dans une société démocratique, lorsque les intérêts des mineurs ou la protection de la vie privée des parties au procès l'exigent, ou dans la mesure jugée strictement nécessaire par le tribunal, lorsque dans des circonstances spéciales la publicité serait de nature à porter atteinte aux intérêts de la justice."

---

351 *In extenso* : W. VAN LAETHEM, 'Problemen met veiligheidsadvies van beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen', *Juristenkrant* 2021, 439, 8-9.

352 Conseil d'État, arrêt n° 251.927, 26 octobre 2021 (www.raadvst-consÉtat.be).

La situation au regard du droit actuel et de la jurisprudence européenne nécessite une réflexion dans l'intérêt du justiciable. Il s'agit, d'une part, de la question de la publication des décisions et, d'autre part, de la question des audiences publiques.

IX.2.4.1. LA PUBLICATION

Déjà fin juin 2014, la Commission de Modernisation de l'Ordre judiciaire (CMOJ) avait abordé cette question.[353] Pour rappel, la Belgique a trois cours suprêmes : la Cour de cassation, le Conseil d'État et la Cour constitutionnelle. Chacune d'entre elles est soumise à un régime différent de publication de ses décisions et chacune en assure de façon autonome la publicité. De manière plus générale, l'accessibilité de la jurisprudence est assurée en Belgique par des banques de données publiques ou privées et par des revues.

Pour le Conseil d'État, la matière est régie par un arrêté royal et un arrêté ministériel.[354] La règle est la publication de tous les arrêts, sous la seule réserve de la matière très spécifique de la législation concernant l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers. Il n'y a donc pas, contrairement à celle de la Cour de cassation, de filtre qualitatif empêchant l'accès à une partie de la jurisprudence. Le Conseil d'État a en effet adopté une double approche dans la publication de ses décisions : d'une part, il met en ligne très rapidement l'ensemble de sa jurisprudence, d'autre part, dans une banque de données séparée, il procède à une sélection raisonnée et structurée des arrêts qu'il estime intéressants. Cette banque de données est publique et gratuite. Le rapport au Roi précédent l'arrêté royal est très éclairant sur l'importance d'assurer l'accessibilité à la jurisprudence de cette juridiction. La question de l'anonymisation est également traitée dans l'arrêté royal lui-même.

Plus fondamentalement, le rapport de la CMOJ constatait le « *déficit démocratique* » qu'engendre cette indisponibilité de la jurisprudence des cours et tribunaux : comment garantir l'accès pour tous à la justice si cette jurisprudence est inaccessible ? Comment enseigner et pratiquer le droit si nul ne sait comment la justice se dit et se fait ?

En ce qui concerne l'Organe de recours, la Loi organique du 11 décembre 1998 ne prévoit aucune disposition à cet égard. Les différentes autorités de sécurité ont exprimé leur inquiétude face à une telle publication.

---

353 Commission de Modernisation de l'Ordre judiciaire, *Rapport consacré à la question de la publication des décisions judiciaires. La plume, le Pélikan et le nuage*, 30 juin 2014.

354 Arrêté royal du 7 juillet 1997 relatif à la publication des arrêts du Conseil d'État et des ordonnances de non-admission du Conseil d'État et Arrêté ministériel du 3 février 1998 déterminant le réseau d'informations accessible au public et le support magnétique en vue de la consultation et de l'enregistrement des arrêts du Conseil d'État.

Le président de l'Organe de recours est bien conscient que sa jurisprudence traite des questions spécifiques et dont certaines pourraient toucher la sécurité des intérêts de l'État. Il est indéniable que l'anonymisation doit être systématique et très prudente à cet égard. La problématique de l'anonymisation est, en Belgique, étroitement liée à celle de la protection de la vie privée dans le cadre des banques de données. Dans le cadre de sa compétence – limitée aux personnes physiques – l'ancienne Commission de protection de la vie privée a suggéré une anonymisation poussée.[355]
L'ouverture par la Chambre des représentants d'un débat sur la publication des décisions de l'Organe de recours n'apparaît-elle pas aujourd'hui comme nécessaire dans le cadre du renforcement démocratique des institutions ?

IX.2.4.2. LES AUDIENCES PUBLIQUES

L'article 6 CEDH consacre le droit à un procès équitable et vise en son alinéa premier notamment la question de la publicité des audiences et du prononcé des décisions à intervenir. Le législateur belge de 1998 n'a pas abordé la question de la publicité des audiences dans la Loi organique sur l'Organe de recours.

Il ressort de l'analyse de la Cour européenne les principes généraux suivants en matière d'audience[356] :
« Le justiciable a, en principe, le droit à une audience publique car cela le protège contre une justice secrète échappant au contrôle du public. Par la transparence qu'elle donne à l'administration de la justice, l'audience publique aide à réaliser le but de l'article 6 § 1 : le procès équitable. Si la tenue d'une audience publique constitue un principe fondamental consacré par l'article 6 § 1, cette obligation n'est pas pour autant absolue (De Tommaso c. Italie [GC], 2017, § 163). Pour déterminer si un procès répond à l'exigence de publicité, il faut envisager la procédure dans son ensemble (Axen c. Allemagne, 1983, § 28).
Dans une procédure se déroulant devant un seul tribunal, le droit de chacun à ce que sa cause soit « entendue publiquement », au sens de l'article 6 § 1, implique le

---

355 Avis n°42/97 du 23 décembre 1997 et recommandation n°03/2012 du 8 février 2012. En 1997, la Commission de la protection de la vie privée écrivait : « *La protection est d'autant plus nécessaire que les outils de navigation et les capacités des systèmes d'information en termes d'interconnexion de données sont de plus en plus puissants et que le contrôle des utilisations opérées à partir de ces interrogations à distance est quasiment inexistant. Ainsi, on peut imaginer la facilité avec laquelle un internaute averti recueillera l'ensemble de la jurisprudence relative à des licenciements pour motifs graves pour en extraire les noms et adresses des employés mis en cause, ou identifiera les médecins dont la responsabilité aurait été mise en cause devant les tribunaux. Le comportement d'un juge face à tel ou tel type de conflits pourra être évalué statistiquement et le nom d'un avocat pourra être associé à un pourcentage d'issues favorables de procès.* » (Avis CPVP n°42/97 du 23 décembre 1997).

356 CONSEIL DE L'EUROPE, COUR EUROPÉENNE DES DROITS DE L'HOMME, *Guide sur l'article 6 de la Convention européenne des droits de l'homme*, 31 décembre 2021 https://www.echr.coe.int/documents/guide_art_6_fra.pdf

droit à une «audience » (Göç c. Turquie [GC], 2002, § 47 ; Fredin c. Suède (no 2), 1994, §§ 21-22 ; Allan Jacobsson c. Suède (no 2), 1998, § 46 ; Selmani et autres c. l'ex-République yougoslave de Macédoine, 2017, §§ 37-39).

La publicité des débats doit également être lue sous l'angle de la question de la présence du public et de la presse : La publicité des débats judiciaires protège les justiciables contre une justice secrète échappant au contrôle du public et constitue ainsi l'un des moyens qui contribue à la préservation de la confiance dans les tribunaux. Elle aide à atteindre le but tenant à l'équité du procès (Martinie c. France [GC], 2006, § 39 ; Diennet c. France, 1995, § 33 ; Gautrin et autres c. France, 1998, § 42 ; Hurter c. Suisse, 2005, § 26 ; Lorenzetti c. Italie, 2012, § 30). L'article 6 § 1 ne fait cependant pas obstacle à ce que les juridictions décident, au vu des particularités de l'affaire, de déroger à ce principe (Martinie c. France [GC], 2006, §§ 40-44). Le huis clos, qu'il soit total ou partiel, doit alors être strictement commandé par les circonstances de l'affaire (Lorenzetti c. Italie, 2012, § 30). Le texte de l'article 6 § 1 prévoit plusieurs exceptions. Selon le libellé de cet article, « l'accès de la salle d'audience peut être interdit à la presse et au public pendant la totalité ou une partie du procès » :

– dans l'intérêt de la moralité, de l'ordre public ou de la sécurité nationale dans une société démocratique » (B. et P. c. Royaume-Uni, 2001, § 39 ; Zagorodnikov c. Russie, 2007, § 26) ;

– lorsque les intérêts des mineurs ou la protection de la vie privée des parties au procès l'exigent » : les intérêts des mineurs ou la protection de la vie privée des parties au procès sont en jeu, par exemple, dans les procédures relatives à la garde d'enfants mineurs à la suite du divorce ou de la séparation des parents, ou lors des litiges entre membres d'une même famille (ibidem, § 38). En revanche, dans les affaires qui concernent le placement d'un enfant dans une institution publique, les raisons de soustraire l'affaire à l'examen du public doivent faire l'objet d'un examen attentif (Moser c. Autriche, 2006, § 97). Dans le cas d'une procédure disciplinaire dirigée contre un médecin, si la nécessité de préserver le secret professionnel ou la vie privée des patients peut motiver le huis clos, celui-ci doit être strictement commandé par les circonstances (Diennet c. France, 1995, § 34). Pour un exemple de procédure dirigée contre un avocat, voir Hurter c. Suisse, 2005, §§ 30-32 ;

– « ou dans la mesure jugée strictement nécessaire par le tribunal, lorsque dans des circonstances spéciales la publicité serait de nature à porter atteinte aux intérêts de la justice » : il est possible de déroger au principe de la publicité des débats pour protéger la sécurité et l'intimité des témoins ou pour favoriser le libre échange d'informations et d'opinions dans la poursuite de la justice (B. et P. c. Royaume-Uni, 2001, § 38 ; Osinger c. Autriche, 2005, § 45).

La Cour a ajouté que la jurisprudence concernant la tenue d'une audience en tant que telle – et visant surtout le droit à s'exprimer devant le tribunal prévu à l'article 6 § 1 – pouvait s'appliquer par analogie s'agissant de la tenue de débats ouverts au public. Ainsi, lorsqu'une audience s'est tenue en vertu du droit national, cette audience doit en principe être publique. La tenue d'une audience publique n'est pas pour autant

absolue, les circonstances qui permettent de s'en dispenser dépendant essentiellement de la nature des questions dont les tribunaux internes se trouvent saisis (De Tommaso c. Italie [GC], 2017, §§ 163-167). Des « circonstances exceptionnelles – et notamment le caractère hautement technique des questions à trancher – peuvent justifier l'absence de publicité, pourvu que la spécificité de la matière n'exige pas le contrôle du public » (Lorenzetti c. Italie, 2012, § 32).
La simple présence de documents classifiés dans un dossier judiciaire n'implique pas automatiquement l'exclusion du public des débats. Ainsi, avant d'exclure le public d'une affaire particulière, le tribunal devrait considérer de manière spécifique si une telle exclusion est nécessaire à la protection d'un intérêt public et la limiter à ce qui est strictement nécessaire pour atteindre l'objectif poursuivi (Nikolova et Vandova c. Bulgarie, 2013, §§ 74-77 au sujet d'un huis clos en raison de documents classés secret d'État ; voir aussi sur les principes, Vasil Vasilev c. Bulgarie, 2021,§§ 105-106). »*

La question de la publicité des audiences mérite une attention particulière et un débat approfondi soumis à la Chambre des représentants. Le président de l'Organe de recours est prêt à participer activement à ce processus.

IX.2.5. EFFECTIVITÉ DES DÉCISIONS DE L'ORGANE DE RECOURS

La question de l'effectivité des décisions de l'Organe de recours se pose à l'égard de l'Autorité nationale de sécurité (ANS). Outre le refus de transmettre des dossiers administratifs dans le cadre de certains recours, le président de l'Organe de recours rappelle le prescrit de l'article 12 § 6 de la Loi organique qui stipule : « *Les décisions de l'organe de recours sont exécutoires de plein droit dès leur notification* ».

C'est ainsi que, dans une affaire, l'Organe de recours avait octroyé à l'intéressé une habilitation de sécurité (niveau SECRET UE) qui lui était refusée par l'ANS. Le 19 juillet 2021, le Tribunal de première instance francophone de Bruxelles (RG 2021/51/C) a, par ordonnance contradictoire, en référé, donné injonction à l'État belge, par l'intermédiaire de l'ANS, de délivrer au requérant son habilitation de sécurité dans le mois de la signification de l'ordonnance sous peine d'une astreinte fixée à 500 euros par jour de retard, avec un maximum de 10.000 euros.

Relevons que dans ce même dossier, les médiateurs fédéraux saisis par l'intéressé en raison de la non-exécution de la décision de l'Organe de recours, étaient intervenus, toujours sans succès. Ils ont classé la plainte comme fondée avec la motivation suivante : *« […] Dans un état de droit, la non-exécution d'une décision prise dans le cadre d'un recours administratif porte une atteinte sérieuse à la sécurité juridique ».*

IX.2.6. PERSPECTIVE

La ministre de la Défense, suivant les recommandations du Comité permanent R, entend déposer des projets de loi visant à systématiser le principe d'une vérification de sécurité tant pour les civils que pour les miliaires de la Défense. Cet avis de sécurité ne serait plus uniquement requis lors de la candidature mais durant toute la vie professionnelle des différents membres de la Défense. On peut supposer que cet avis de sécurité sera renouvelé tous les cinq ans. Les éventuels recours seront en principe de la compétence de l'Organe de recours.

À la suite de l'enquête de contrôle de septembre 2021 du Comité permanent R sur la manière dont la Sûreté de l'État a assuré le suivi de la commissaire du gouvernement Ishane Haouach, celui-ci avait recommandé que l'exercice de certaines « fonctions publiques » requiert la vérification préalable de l'intégrité, de la loyauté et de la discrétion, comme l'exige la législation en vigueur dans certains pays européens. La mise en œuvre de cette recommandation devrait entraîner une extension des avis de sécurité qui eux aussi feront l'objet d'un contrôle juridictionnel de l'Organe de recours.

La question de la franchise postale devrait être rencontrée tout comme la possibilité d'introduire un recours par voie digitale et de permettre les actes de notification, suivant la préférence du justiciable, par voie postale ou digitale pour la procédure pendante devant l'Organe de recours.

CHAPITRE X.
LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R

X.1. COMPOSITION DU COMITÉ PERMANENT R

La composition du Comité est restée identique en 2021 : Serge Lipszyc (F), premier substitut de l'auditeur du travail près de l'auditorat du travail de Liège, a continué à remplir sa mission de président. Pieter-Alexander De Brock (N), et Thibaut Vandamme (F), substitut du procureur du Roi de l'arrondissement du Luxembourg, ont exercé leur mandat de membre.[357] [358]

En attendant la nomination d'un greffier, Wauter Van Laethem (N) a été désigné comme greffier faisant fonction.[359]

Plusieurs changements sont également intervenus au sein du services d'Enquêtes, dont la direction est assurée par Fabian Poncelet (F) depuis le 1er janvier 2021. Un nouveau commissaire-auditeur francophone a rejoint les rangs du service en juin 2021. Il est détaché de la Police fédérale. Un commissaire-auditeur a remis sa démission et sera remplacé dans le courant de l'année 2022.

Enfin, le cadre administratif du Comité permanent R a lui aussi subi quelques changements. Le juriste, recruté en décembre 2020, et en fonction à la Section documentation et analyse juridique, a repris ses fonctions dans son service d'origine en août 2021. Deux attachés francophones ont rejoint les rangs de cette

---

357 Thibaut Vandamme a prêté serment le 11 janvier 2021. En application de l'article 157, paragraphe 6, du règlement de la Chambre, lors de la séance plénière du 20 mai 2021, Thierry Werts a été désigné comme premier suppléant de Thibaut Vandamme (CRABV55PLEN105, 20 mai 2021, 46).

358 Fin 2021, Wauter Van Laethem a remis sa démission en tant que deuxième suppléant du conseiller néerlandophone (*C.R.I.* Chambre 2021-2022, 10 novembre 2021 CRIV55PLEN139, 68). Il a été remplacé en mars 2022 par Filip Vanneste, substitut du procureur général près la Cour d'appel d'Anvers (*C.R.I.* Chambre 2021-2022, 24 mars 2022, CRIV55PLEN171, 67).

359 Un appel à candidature pour le poste de greffier du Comité permanent R est paru à la mi-mai 2020 au Moniteur belge. Le 21 juin 2021, un projet de loi a été déposé pour élargir les conditions de nomination des greffiers respectifs des Comités permanents R et P (*Doc.Parl.* Chambre 2020-21, 55K2064/001). La question a d'abord été examinée en Conférence des présidents (24 février et 3 mars 2021) (*Doc.Parl.* Chambre 2020-21, 55K1924/001). La 'loi du 14 août 2021 modifiant la loi organique du 18 juillet 1991 [...], et visant à élargir les conditions de nomination des greffiers du Comité R et du Comité P' a été publiée au Moniteur belge le 8 décembre 2021. Une nouvelle vacance est parue au Moniteur belge le 19 juillet 2021. Le 26 avril 2022, Frédéric Givron (F) a prêté serment en présence de la Présidente de la Chambre en tant que nouveau Greffier du Comité permanent R.

section en octobre 2021. En avril 2021, une secrétaire statutaire néerlandophone a été recrutée. Fin 2021, le cadre administratif comptait 18 collaborateurs.

À la mi-juin 2021, le président du Comité permanent R s'est à nouveau adressé à la Présidente de la Chambre des représentants concernant le manque de personnel et l'augmentation considérable de tâches assignées au Comité.[360] Malgré le dynamisme dont fait preuve la Chambre dans le cadre des objectifs de synergie, auxquels le Comité apporte son soutien, le Comité a jugé nécessaire de solliciter un renfort urgent. Il n'est en effet pas en mesure de mener à bien toutes les missions légales ni de répondre de manière adéquate aux différentes demandes formulées par la Chambre.

X.2. UN AUDIT RELATIF AU BIEN-ÊTRE AU COMITÉ

À la suite des signes de malaise au sein du Comité permanent R, il a été décidé de charger IDEWE, un service externe de prévention et de protection au travail, d'effectuer une analyse des risques psychosociaux. L'audit a analysé des thèmes correspondant aux cinq domaines des risques psychosociaux au travail (contenu du travail, organisation du travail, environnement de travail, conditions de travail et relations interpersonnelles au travail). En a résulté un rapport complet[361] détaillant les résultats de l'analyse et formulant un avis à l'employeur.[362]

Prenant appui sur cet audit, un processus de changement a été initié. Le Comité permanent R sera guidé par le SPF Stratégie et Appui. Le projet comprend une enquête auprès des *stakeholders*, une analyse SWOT et une analyse PESTEL[363] approfondies. Le projet devrait être achevé à la fin du mois de juin 2022.

Suite aux résultats de l'audit, une nouvelle personne de confiance néerlandophone a été nommée à la mi-décembre 2021. La nomination d'une personne de confiance francophone a suivi à la fin du mois de janvier 2022.[364]

---

360 Lettre du Président du Comité permanent R à la Présidente de la Chambre des représentants datée du 16 juin 2021.

361 IDEWE, Analyse des risques psychosociaux, 23 novembre 2021, 30 p.

362 Le modèle 'd'efficacité collective' (SDRPI) a été utilisé pour traiter les problèmes identifiés. Ce modèle se concentre sur le **S**ystème (contexte dans lequel le travail est effectué), les **O**bjectifs (fixation d'objectifs clairs et partagés), les **R**ôles (ce que l'on peut attendre de chacun), les **P**rocédures (développement de pratiques appropriées) et les **R**elations interpersonnelles.

363 L'analyse PESTEL est un modèle d'analyse de stratégie d'entreprise utilisé pour identifier l'influence des facteurs externes sur une organisation. L'acronyme PESTEL renvoie aux facteurs politiques, économiques, sociologiques, technologiques, environnementaux et légaux.

364 La législation (2014) sur les risques psychosociaux au travail impose aux personnes de confiance de suivre une formation de base de 30 heures. L'employé est tenu de suivre la formation dans les deux ans suivant sa nomination en tant que personne de confiance.

X.3. RÉUNIONS AVEC LA COMMISSION DE SUIVI

La composition de la Commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de Contrôle des services de police et du Comité permanent de Contrôle des services de renseignement et de sécurité (la Commission de suivi) a connu quelques changements en 2021. En étaient membres avec voix délibérative Peter Buysrogge (N-VA), Joy Donné (N-VA), Cécile Thibaut (Ecolo-Groen)[365], Stefaan Van Hecke (Ecolo-Groen), André Flahaut (PS), Ahmed Laaouej (PS), Ortwin Depoortere (VB), Marijke Dillen (VB), Denis Ducarme (MR), Servais Verherstraeten (CD&V), Nabil Boukli (PVDA-PTB), Patrick Dewael[366] (Open Vld) et Bert Moyaers (Vooruit). La Présidente de la Chambre, Eliane Tillieux (PS), assume la présidence de la Commission. Georges Dallemagne (Les Engagés) participe en tant que membre sans voix délibérative.

Dans le courant de l'année 2021, et malgré la crise sanitaire, plusieurs réunions (neuf au total) ont eu lieu avec la Commission. Lors de ces réunions, tenues à huis clos, plusieurs enquêtes de contrôle que le Comité permanent R avait clôturées ont été discutées.[367] Fin avril et début juillet 2021, des réunions ont eu lieu avec le Comité permanent P pour discuter respectivement de l'enquête de contrôle conjointe relative à l'Organe de coordination pour l'analyse de la menace (OCAM) et ses services d'appui, et de l'enquête de contrôle conjointe relative au rôle de l'OCAM dans le suivi de Jürgen Conings. Du temps a également été consacré au rapport rédigé dans le cadre de la compétence de contrôle partagée avec l'Organe de contrôle de l'information policière (C.O.C.) concernant les banques de données (art. 44/6 LFP). Lors de la réunion du 22 septembre 2021, le *Rapport d'activités 2020* du Comité permanent R a été discuté.[368] La Commission a notamment souligné *'l'importance d'un rapport annuel, non seulement pour rendre compte des activités du Comité R au parlement, mais également pour informer les personnes extérieures en toute transparence (professeurs, journalistes, personnel des services de renseignement, ...)'*. Une série de thématiques ont particulièrement retenu l'attention des Députés telles que le suivi des plaintes, le Memorandum of Understanding (MoU) entre le SGRS et les services de renseignement rwandais, le COVID-19 et le rôle des services de renseignement, ou encore les interceptions étrangères. En guise de

365 Remplacée depuis lors par Julie Chanson (Ecolo-Groen).

366 Remplacé depuis lors par Tim Vandeput (Open Vld).

367 Une réunion s'est tenue avec comme point à l'agenda notamment le rapport intermédiaire (état des lieux) de l'enquête de contrôle relative à Jürgen Conings.

368 La Commission se réfère à cet effet à l'article 66*bis*, § 3,1° L.Contrôle, tel que modifié par la loi du 6 janvier 2014 modifiant diverses lois de réformes institutionnelles, *M.B.* 31 janvier 2014.

conclusion, la Commission a pris *'acte du Rapport d'Activités 2020 du Comité R et souscrit à ses recommandations*.[369]

Enfin, la Commission s'est également penchée sur les problèmes internes à la tête du Comité permanent R.[370] Trois réunions de la Commission ont été organisées, à huis clos, à l'automne 2021.

X.4. RÉUNIONS COMMUNES AVEC LE COMITÉ PERMANENT P

Sans compter les quelques contacts (informels), aucune réunion commune ne s'est tenue en 2021 avec le Comité permanent P.[371]

Trois enquêtes communes ont été effectuées en 2021 : l'enquête de suivi sur la mise en œuvre des recommandations émises par les Comités permanents R et P dans le cadre de l'enquête sur les services d'appui de l'OCAM (cf. I.1) et l'enquête de contrôle sur les quatre services d'appui 'supplémentaires' de l'OCAM (cf. I.2). La troisième enquête commune portait sur 'le rôle de l'OCAM dans le suivi du militaire Jürgen Conings' (cf. I.10). À cette fin, les services d'appui des deux Comités ont coopéré activement.

Les deux Comités ont chargé leurs services d'Enquêtes respectifs de préparer des procédures de travail pour le traitement des plaintes et des enquêtes de contrôle conjointes. Le Comité permanent P a également accepté la demande du Comité permanent R, et plus particulièrement de son service d'Enquêtes, d'obtenir une formation dans le cadre de la consultation de la Banque de données nationale générale (BNG).[372] Enfin, conformément à l'art. 52 L.Contrôle, les rapports d'activités et les rapports d'enquêtes de contrôle ont été échangés.

---

369 *Doc. parl.* Chambre 2020-21, 55K2209/01, 20 octobre 2021 (Rapport d'activités 2020 du Comité permanent de Contrôle des services de renseignement et de sécurité, Rapport fait au nom de la commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de Contrôle des services de police et du Comité permanent de contrôle des services de renseignement et de sécurité).

370 La Commission s'est notamment réunie suite à la parution d'un article publié à la suite de l'affaire Jürgen Conings (Q. JARDON, 'Serge Lipszyc. Gendarme des services secrets, *Wilfried*, Automne 2021, n° 17, 1-7) et une demande introduite auprès de la Présidente de la Chambre par les deux conseillers.

371 Art. 52 L.Contrôle prévoit qu'au minimum deux réunions communes doivent s'organiser chaque année.

372 En octobre 2017, le Comité permanent R a signé un protocole d'accord avec la Police fédérale concernant l'application de l'arrêté royal du 30 octobre 2015 relatif à l'accès direct du Comité permanent de contrôle des services de renseignement et de sécurité et de son Service d'enquêtes aux données et informations de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police (*M.B.* 20 novembre 2015).

X.5. UNE ATTENTION MÉDIATIQUE IMPORTANTE

Le Comité permanent R a fait l'objet d'une attention médiatique importante en 2021, ce qui dénote des années précédentes. Quatre événements (repris en ordre chronologique) en sont principalement à l'origine :

Tout d'abord, la publication du rapport de l'enquête de contrôle relative au suivi opéré par les services de renseignements de la menace posée par l'extrême droite.[373] Les principales conclusions ont été partagées par plusieurs médias belges.

L'affaire Jürgen Conings et le rôle occupé par le Comité ont ensuite été largement médiatisés. Pour rappel, le Comité a été chargé par la ministre de la Défense de réaliser une enquête de contrôle afin de vérifier notamment la fiabilité des informations relatives aux personnes suspectées de radicalisation au sein de la Défense, de formuler des recommandations en vue de garantir le bon fonctionnement du SGRS ainsi que de la Défense dans son ensemble.[374] Les conclusions de ce rapport (très attendu) ont été largement relayées par les médias.

Le Comité permanent R a également été saisi dans l'affaire Haouach, ancienne commissaire de gouvernement auprès de l'Institut pour l'égalité entre les femmes et les hommes.[375] Cette affaire a fait l'objet d'une importante attention médiatique suite aux allégations dans la presse faisant état de l'existence d'une note de la VSSE évoquant des 'contacts étroits' entre les Frères musulmans et la commissaire de gouvernement, à l'insu ou non de cette dernière.

Enfin, est parue en octobre 2021 l'interview accordée par le président du Comité à la revue *Wilfried (supra)*. Dans cette interview, le président exprimait certaines inquiétudes personnelles suite à plusieurs événements et dossiers marquants tels que l'affaire Jürgen Conings. Cette interview, les réactions à celle-ci, ainsi que les tensions au sein de la direction du Comité qui s'en sont suivies, ont retenu l'attention des médias.

Le Comité est conscient que la communication sur ses missions constitue un enjeu complexe mais ô combien essentiel. Il ambitionne d'y prêter une attention plus grande à l'avenir, en améliorant notamment la mise à disposition des informations. La révision future de son site internet s'inscrit pleinement dans cette démarche.

X.6. LE 'DATA PROTECTION OFFICER' AU COMITÉ

Un *Data Protection Officer* (DPO) est nommé depuis plusieurs années au sein du Comité, pour tous les traitements de données à caractère personnel qui ne relèvent

---

373 COMITÉ PERMANENT R, *Rapport d'activités 2020*, 38 et s. ('I.7. Le suivi de l'extrême droite par les services de renseignements belges').

374 À ce propos, 'I.9. La détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings.'

375 À ce propos, voir 'I.11. Le suivi d'un commissaire de gouvernement par la VSSE'.

pas de la «sécurité nationale». Dans le cadre de l'exercice de synergie réalisé par la Chambre des représentants, le DPO remplit également cette fonction pour d'autres institutions à dotation situées dans le bâtiment du Forum. Le *Data Protection Officer* a fourni des conseils sur la surveillance par caméra pour laquelle un registre a été établi et la déclaration formalisée suite à la 'nouvelle loi caméras'[376]. En outre, le DPO a également fourni des conseils et des informations sur la gestion interne des données à caractère personnel des membres du personnel, notamment dans le contexte de la pandémie de COVID-19.

X.7. MOYENS FINANCIERS ET ACTIVITÉS DE GESTION

Le budget 2021 du Comité permanent R a été fixé à 5,215 millions d'euros, ce qui représente une augmentation de 13 % par rapport à 2020.[377]

La principale raison de cette augmentation provient en grande partie de la présentation d'un projet opérationnel de digitalisation des processus de travail. Ce projet était présenté en partenariat avec un opérateur industriel coutumier des administrations publiques et habitué à leurs procédures administratives. Bien qu'adhérant aux principes présentés par le Comité, la Commission de la Comptabilité a cependant décidé de geler le processus de gestion documentaire dans l'attente de conclusions des concertations en cours entreprises entre les services de la Questure et le Comité afin que le projet puisse être intégré dans les synergies éventuelles.

Les sources de financement attribuées par la Chambre des représentants[378] sont les suivantes : 74,44 % au titre du budget de dotation et 25,56 % de boni de 2019.

L'exécution du budget 2021 a produit un boni comptable de 1,87 millions d'euros (chiffres non-audités) euros, représentant la différence entre le budget approuvé et les dépenses constatées.

Le budget est composé de différentes sources de financement dont le seul apport en termes de trésorerie nette est constitué par la dotation inscrite au budget général de l'État. Jusqu'en 2017, cette dotation ne suffisait pas à couvrir les dépenses réelles du Comité, ce qui générait une perte structurelle. La tendance à appliquer autant que possible l'article 57 alinéa 1er L.Contrôle (qui stipule que les crédits de fonctionnement sont inscrits au budget des dotations) permet à ce jour au Comité de financer ses activités.

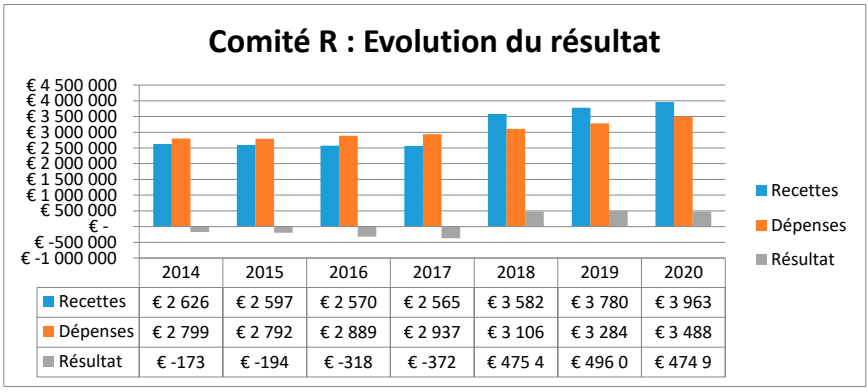
---

376 Loi du 30 juillet 2018 modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, en vue d'améliorer la cohérence du texte et sa conformité avec le Règlement général sur la protection des données (RGPD), *M.B.* 31 août 2018.

377 *C.R.I.* Chambre 2020-21, 17 décembre 2020, PLEN 081, 63.

378 *Doc. parl.* Chambre 2020-21, 55-1676/001, 30-34.

Le dégagement d'un boni comptable considérable provient essentiellement de l'écart temporel existant entre l'approbation des budgets et l'entrée effective en service du personnel à cause de la longueur des procédures de recrutement et de l'obtention des habilitations de sécurité requises. Cette tendance a été particulièrement marquée pendant l'exercice 2021, où le Comité a été confronté à plusieurs phénomènes concomitants tels que le départ à la retraite de plusieurs membres du personnel et les retards enregistrés dans le remplacement de ces personnes. On peut affirmer que 2021 a connu un *turnover* important dans les effectifs de chaque catégorie de personnel tant au niveau managérial qu'au niveau opérationnel : ainsi, le poste de greffier est resté vacant durant toute l'année jusqu'à désignation récente d'un successeur par la Chambre des représentants (voir *supra*). D'autres postes ont également été affectés par des choix de carrière différents de la part de leurs titulaires. Cela, cumulé au gel du budget affecté au projet de digitalisation (*voir supra*) décidé par la Chambre, a généré un boni important qui sera probablement réaffecté au budget de fonctionnement 2023 lors de l'examen des propositions budgétaires par la Chambre des représentants.



	2014	2015	2016	2017	2018	2019	2020
Recettes	€ 2 626	€ 2 597	€ 2 570	€ 2 565	€ 3 582	€ 3 780	€ 3 963
Dépenses	€ 2 799	€ 2 792	€ 2 889	€ 2 937	€ 3 106	€ 3 284	€ 3 488
Résultat	€ -173	€ -194	€ -318	€ -372	€ 475 4	€ 496 0	€ 474 9

À partir de l'exercice 2023, le Comité sera pleinement intégré dans le projet de mise en place de Synergies initié par la Chambre (voir *infra*)[379] qui auront des impacts indéniables sur le fonctionnement des organes à dotation en général et du Comité permanent R en particulier. Ces changements auront un effet sur le cadre du personnel et sur les crédits de fonctionnement qui seront mutualisés dans la mesure du possible. La date-pivot d'entrée en application de ces modifications a été fixée au 1er janvier 2023.

379 *Doc. parl.* Chambre 2020-21, 55-1924/001.

X.8. MISE EN ŒUVRE DES RECOMMANDATIONS DE L'AUDIT DE LA COUR DES COMPTES

À la demande de la Commission de la Comptabilité de la Chambre des représentants, la Cour des comptes a, dès 2017, initié une enquête sur les institutions à dotation, conjointement à Ernst & Young.[380] Le rapport d'audit, transmis fin mars 2021, reprenait des recommandations concernant les 'missions' des neuf institutions à dotation concernées par l'audit, dont le Comité permanent R. [381]

Entre janvier et début février 2021, les services de la Questure et le secrétariat de la Commission ont auditionné les institutions concernées, parmi lesquelles le Comité permanent R.

En avril 2021, un accord a été trouvé au sein de la Commission de la Comptabilité sur les synergies à initier entre les institutions concernées. Il s'agit notamment de mettre en place un centre de services partagés (Incentris) et un portail citoyen. Il a également été décidé d'harmoniser les statuts du personnel et les barèmes des institutions concernées ainsi que de rationaliser le parc automobile des institutions. Une réorganisation de certains locaux, notamment ceux du Comité permanent R, afin d'y accueillir la Commission BIM, est aussi envisagée. Pour concrétiser ces orientations, des groupes de travail thématiques ont été mis en place auxquels participent des membres de la Chambre ainsi que de certaines institutions, la logique étant qu'il ait une représentation par 'famille' d'institutions (une famille étant constituée d'institutions aux missions apparentées).[382] [383]

En septembre 2021, une réunion a été organisée par la Chambre à destination des membres du personnel des institutions concernées afin d'informer ces derniers des orientations décidées pour maximiser les synergies et l'état d'avancement des projets visant à les concrétiser.

Afin d'étudier la possibilité d'allouer une partie des locaux du Comité permanent R à la Commission BIM, plusieurs visites des locaux du Comité permanent R ont été organisées à partir d'octobre 2021 en présence de l'architecte de la Chambre. Des réunions se sont également tenues avec la Commission BIM,

---

380 La Cour des comptes s'est surtout concentrée sur les aspects budgétaires (une analyse des recettes et des dépenses) et sur la délimitation des missions des différentes institutions. De son côté, Ernst & Young était principalement chargé de procéder à une analyse approfondie des processus, des systèmes et de l'organisation de chacune de ces institutions.

381 *Institutions à dotation. Missions – Recettes– Dépenses.* Audit réalisé à la demande de Commission de la Comptabilité de la Chambre des représentants, Rapport approuvé le 28 mars 2018 par l'assemblée générale de la Cour des comptes.

382 Le Comité permanent R appartient à la famille « Sécurité et protection » à laquelle appartiennent également le Comité permanent P, l'Autorité de protection des données, le C.O.C. et la Commission BIM.

383 A la mi-octobre 2021, la Présidente de la Chambre a demandé au Comité de participer plus activement et de veiller à un flux d'informations efficace afin de permettre aux groupes de travail mis en place dans le cadre du projet 'synergie entre les institutions à dotation' de remplir adéquatement leurs tâches. La Présidente s'est dit consciente que l'absence de greffier pouvait complexifier les choses.

le Comité permanent R et ce même architecte afin d'évaluer les implications et les coûts d'un tel projet. Un dossier sera remis dans le courant de l'année 2022 à la Commission de la Comptabilité amenée à se prononcer sur un déménagement effectif de la Commission BIM.

X.9. FORMATIONS

Compte tenu de l'intérêt pour l'organisation, le Comité permanent R encourage ses membres et ses collaborateurs à suivre des formations générales (en informatique, en management, etc.) ou propres au secteur, ou encore à participer à des conférences.[384] En raison des mesures adoptées dans le cadre de la crise sanitaire, il n'a pas été possible de suivre des formations internes ou externes en 2021.

[384] Les briefings de sécurité auxquels les collaborateurs sont tenus d'assister ont, quant à eux, bien eu lieu.

CHAPITRE XI.
RECOMMANDATIONS

À la lumière des enquêtes de contrôle, des contrôles et des inspections clôturés en 2021, le Comité permanent R formule les recommandations reprises ci-après. Ces recommandations portent à la fois sur la protection des droits que la Constitution et la loi confèrent aux personnes, sur la coordination et l'efficacité des services de renseignement, de l'Organe de coordination pour l'analyse de la menace (OCAM) et des services d'appui ainsi que sur l'optimalisation des possibilités d'enquête du Comité permanent R.

XI.1. RECOMMANDATIONS RELATIVES À LA PROTECTION DES DROITS QUE LA CONSTITION ET LA LOI CONFÈRENT AUX PERSONNES

XI.1.1. RÉDACTION D'UNE PROPOSITION DE DIRECTIVE SUR LA COMMUNICATION D'INFORMATIONS PAR LA VSSE OU LE SGRS AUX EMPLOYÉS ET ADAPTATION DES DIRECTIVES EXISTANTES[385]

Le Comité a recommandé que la Sûreté de l'État (VSSE) et le Service Général du Renseignement et de la Sécurité (SGRS), dans les six mois suivant la conclusion de l'enquête de contrôle intitulée '*L' échange d'informations sur un collaborateur entre les services de renseignement et un employeur privé ou public*', rédigent une proposition de directive visant à mettre en œuvre la dernière partie de phrase de l'article 19, alinéa 1er L.R&S à l'attention des ministres de la Justice et de la Défense, en leur demandant de soumettre la proposition au Conseil national de sécurité pour approbation.

La VSSE doit en outre évaluer ses directives en la matière et les adapter au cadre légal. Compte tenu de l'importance de cette matière, cette adaptation doit également avoir lieu dans un délai de six mois.

Par ailleurs, le Comité recommande au législateur de préciser si l'article 19, alinéa 1er, dernière phrase L.R&S contient également une obligation, dans certains

[385] Voir Chapitre 'I.3. L'échange d'informations sur un collaborateur entre les services de renseignement et un employeur privé ou public'.

cas, de répondre à une question ou de fournir des informations d'initiative. Dans l'attente d'une initiative législative, cette question doit être réglée dans la directive du Conseil national de sécurité.

XI.1.2. DIRECTIVES EN MATIÈRE DE SUIVI DE MANDATAIRES POLITIQUES[386]

Le Comité permanent R réitère avec insistance sa recommandation précédente remontant à 2013, selon laquelle le SGRS doit établir des directives claires quant au recueil, au traitement, à la consultation, au stockage et à l'archivage des données des mandataires politiques.

Le Comité permanent R recommande également que les services de renseignement accordent, dans leurs rapports, l'attention nécessaire à la position d'une personne mentionnée dans un rapport vis-à-vis de la menace (victime, acteur, passant, etc.)

XI.2. RECOMMANDATIONS RELATIVES À LA COORDINATION ET À L'EFFICACITÉ DES SERVICES DE RENSEIGNEMENT, DE L'OCAM ET DES SERVICES D'APPUI

XI.2.1. RECOMMANDATIONS RELATIVES À L'OCAM ET SES (NOUVEAUX) SERVICES D'APPUI[387]

Une (in)formation pour les membres du personnel de la Direction Générale des Établissements Pénitentiaires détachés auprès de l'OCAM

Il a été constaté que les membres détachés de Direction générale des Établissements Pénitentiaires (DG EPI) ne se déplacent que peu, voire pas du tout, au sein de leur service d'origine et disent ne pas être mis au courant des changements qui pourraient s'y opérer. Une (in)formation régulière leur permettant de connaître les changements éventuels (législatifs ou d'ordre interne par exemple) au sein de leur service d'origine serait une plus-value.

386 Voir Chapitre 'I.8. Enquête de contrôle sur le suivi des mandataires politiques'

387 Voir Chapitres 'I.1 Les services d'appui de l'OCAM (suivi)' et 'I.2. L'OCAM et les services d'appui supplémentaires'

BINII pour la DG EPI et le Service des Cultes et de la Laïcité

Il serait opportun que le SPF Justice dispose du système BINII (*Belgian Intelligence Network Information Infrastructure)* dans les plus brefs délais afin de permettre aux deux services d'échanger des informations classifiées.

Accès de la Trésorerie aux BDC

Il serait opportun que la Trésorerie dispose au plus vite de ses accès aux Banques de données communes (BDC).

Une boîte mail fonctionnelle pour le Service des Cultes et de la Laïcité

Il serait opportun que le Service des Cultes et de la Laïcité dispose d'une boîte mail fonctionnelle, laquelle permettrait de garantir un suivi de tous les échanges et documents par l'ensemble des membres de la cellule « terrorisme et radicalisme ».

Un accès aux BDC pour le Service des Cultes et de la Laïcité conforme au cadre légal

Il a été constaté que le Service des Cultes et de la Laïcité disposait d'un accès plus large à la Banque de données commune 'Propagandistes de haine' (BDC PH) que ce que prescrit l'AR PH. L'Organe de contrôle de l'information policière (C.O.C.) et le Comité permanent R ont invité les responsables du traitement à mettre un terme aux accès irréguliers et ont recommandé à la Police fédérale d'apporter les solutions techniques nécessaires pour mettre l'accès de ce service en conformité avec la législation en vigueur (soit accès indirect à la BDC PH uniquement). Le C.O.C. et le Comité permanent R ont recommandé par ailleurs aux responsables de traitement d'évaluer, sur les plans juridique et opérationnel, si la règlementation de l'accès du Service des Cultes et de la Laïcité devait (ou non) être révisée.

XI.2.2. APPLICATION CONFORME DE LA POSSIBILITÉ D'INTRODUIRE DES DEMANDES DE SCREENINGS DE SÉCURITÉ[388]

Le Comité invite les acteurs des secteurs publics et privés à examiner si certaines menaces potentielles ne peuvent pas être évitées en recourant, pour certaines fonctions, autorisations ou permis, au système de screening de sécurité prévu

[388] Voir Chapitre 'I.3. L'échange d'informations sur un collaborateur entre les services de renseignement et un employeur privé ou public'.

dans la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (L.C&H). Le Comité insiste toutefois sur un recours judicieux, donc non débridé, à ce système.

XI.2.3. SIGNALEMENT OBLIGATOIRE AUPRÈS DE L'EMPLOYEUR EN CAS DE REPRISE DANS UNE BANQUE DE DONNÉES COMMUNE[389]

Le Comité suggère d'examiner s'il serait utile de prévoir une notification obligatoire à l'employeur pour chaque collaborateur (ou candidat à un emploi) figurant dans la Banque de données commune Terrorist Fighters ou Prédicateurs de haine.

XI.2.4. UN DÉBAT ÉTENDU SUR LES TÂCHES ET PRIORITÉS DES SERVICES DE RENSEIGNEMENT[390]

Le Comité permanent R recommande qu'un débat sociétal (parlementaire) plus large soit mené sur les missions attribuées aux deux services de renseignement dans la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité ainsi que sur les priorités associées. Ceci nécessitera une discussion étayée scientifiquement, ou 'stratégiquement', car il n'y a actuellement pas de méthode scientifique à cet effet sur l'octroi des capacités et moyens suffisants pour permettre à chacun des services de détecter, suivre et maîtriser comme il se doit toutes les menaces contre la sécurité (inter)nationale. Les services de renseignement et de sécurité doivent retenir l'attention du Parlement, et ce pas uniquement au moment où des problèmes individuels surviennent (politique du chalumeau).

XI.2.5. PLUS DE SCREENINGS DE SÉCURITÉ DES MILITAIRES ET DES CIVILS À LA DÉFENSE[391]

Le Comité permanent R a constaté que, sauf à considérer que la carrière de l'intéressé impose une modification du niveau de sécurité, un militaire du département de la Défense ne subit qu'un seul screening de sécurité durant l'entièreté de sa carrière militaire. Pourtant, il apparaît que l'intégrité de certains

---

389 *Ibid.*

390 Voir Chapitres 'I.5. Le suivi des organisations sectaires nuisibles et des organisations criminelles par la Sûreté de l'État' et 'I.9. Enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings'. Un niveau de priorité très élevé a été attribué à cette recommandation.

391 Voir Chapitre 'I.7. Le screening de sécurité des militaires et des civils à la Défense'.

militaires peut effectivement poser problème sur la base de leurs activités entreprises ultérieurement notamment. Cela signifie que ces militaires ne seront connus comme tels que lorsqu'ils représenteront une menace qui aura été détectée par le SGRS.

Le Comité a relevé que les civils du département de la Défense, à de rares exceptions près, ne font l'objet d'aucune vérification de sécurité. Cette différence de traitement ne peut se justifier que si l'usage inapproprié de la fonction qu'ils occupent n'est pas susceptible de menacer les intérêts fondamentaux de l'État. Le Comité recommande par conséquent que l'autorité administrative compétente analyse si la possibilité créée par la Loi du 23 février 2018 de demander des vérifications de sécurité doit être activée. Cette loi permet après une analyse de risque, une analyse de la menace et une analyse d'impact de déteminer les fonctions pour lesquelles il est indiqué d'exiger un avis de sécurité.

La loi permet également qu'une telle évaluation soit effectuée tous les cinq ans et qu'un avis positif soit transformé en avis négatif dans l'intervalle. En ce sens, cette loi offre une possibilité intéressante qui ne s'applique pas actuellement au personnel militaire ; celui-ci ne peut être contrôlé qu'une seule fois (c'est-à-dire au moment de son recrutement). Il faut toutefois garder à l'esprit que l'actuel «avis négatif» pour les militaires implique une «décision négative» *de facto*, alors qu'en vertu de la loi de 2018, les conséquences d'un «avis négatif» reviennent à l'autorité qui a demandé l'avis.

Le Comité a constaté que les étudiants de l'École Royale Militaire (ERM) et d'autres écoles qui dépendent du département de la Défense, à l'inverse des militaires, et à quelques exceptions près, ne sont pas soumis à une vérification de sécurité lors de leur recrutement. Cette différence de traitement n'est pas justifiée et elle présente un risque pour le département de la Défense qui recrute du personnel sans avoir pu idéalement identifier les individus pouvant représenter une source de menace ou ne disposant pas des qualités morales nécessaires à l'exercice de leurs fonctions.

Le Comité a relevé que les étudiants étrangers de l'ERM ne sont pas soumis à une vérification de sécurité lors de leur admission. Cela devrait être précédé d'une analyse de risque systématique et préalable réalisée par le SGRS pour chaque candidat.

Ces recommandations devraient être appliquées à toutes les écoles qui dépendent du département de la Défense.

XI.2.6. LA MISE EN PLACE D'UN ENSEMBLE COHÉRENT 'RENSEIGNEMENT'[392]

Le Comité permanent R recommande la création d'un « ensemble cohérent renseignement » à la Défense reprenant l'entièreté des fonctions militaires de renseignement et permettant de former et de valoriser de manière continue le personnel qui s'y retrouve. Ceci doit permettre de disposer de personnel militaire de qualité et formé au SGRS. Cet ensemble doit disposer d'un maximum d'autonomie en matière de gestion et valorisation de son personnel. Cette recommandation est fondamentale et soulignée depuis de nombreuses années par le Comité.

XI.2.7. STABILITÉ DANS LA GESTION DU PERSONNEL AU SEIN DU SGRS

Le Comité permanent R recommande également d'instaurer une stabilité dans la mise en place de personnel militaire et d'éviter un 'turnover' beaucoup trop fréquent, tel que celui que l'on retrouve ailleurs à la Défense. Une stabilité de cinq ans doit être visée pour les fonctions clés.

XI.2.8. LA VALIDATION DU PLAN DIRECTEUR DU RENSEIGNEMENT (ET DE SÉCURITÉ)

Le Comité permanent R recommande que le Plan Directeur du Renseignement (et de Sécurité) soit validé sans délai. Et le Comité de recommander que ce Plan soit approuvé et évalué chaque année et qu'il soit soumis à l'approbation du ministre de la Défense. Ce plan stratégique définit, en fonction des obligations légales et des missions du SGRS, les moyens nécessaires à mettre en place et, en tenant compte de ceux-ci, les priorités accordées.

XI.2.9. UNE MEILLEURE COMMUNICATION INTERNE AU SGRS

Le Comité permanent R recommande que le SGRS communique mieux avec son personnel pour le familiariser davantage avec la structure et les flux d'informations qui s'y rapportent avant d'envisager des modifications. Il ne sert à rien de remettre

[392] Les recommandations reprises aux points XI.2.6 à XI.2.16. sont issues de l'enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings (Chapitre I.9.). Un niveau de priorité très élevé a été attribué à ces recommandations.

l'ensemble des réalisations en question, mais bien de veiller à l'ancrage de la nouvelle structure où cela s'avère nécessaire. Le Comité était néanmoins conscient que la période du Covid n'a pas facilité la communication en interne, pourtant primordiale pour le lancement d'une nouvelle structure.

XI.2.10. UNE MEILLEURE COMMUNICATION ENTRE LE SGRS ET LES AUTRES AUTORITÉS EN CAS D'INFRACTIONS JUDICIAIRES OU PÉNALES

Le Comité permanent R recommande d'évaluer les canaux et les procédures de communication, tant avec les autorités disciplinaires au sein de la Défense qu'avec les services de police et les autorités judiciaires. Le SGRS doit toujours être informé à temps des mesures administratives (les mises en observation, etc.), décisions (mises sous mandat d'arrêt, inculpations, etc.) et condamnations pénales relatives à un membre du personnel de la Défense. Ce genre de communication doit systématiquement avoir lieu afin que les mesures à prendre puissent être envisagées, plus précisément concernant les habilitations de sécurité.

XI.2.11. UNE MEILLEURE COMMUNICATION INTERNE DU SGRS VERS LE COMMANDEMENT ET LE MINISTRE DE LA DÉFENSE

Le Comité permanent R recommande que le SGRS établisse des directives internes précises quant au flux de communication d'informations vers le commandement et le ministre de la Défense. Ce flux d'informations doit être standardisé, précis et contenir les informations nécessaires à la prise de décision au plus haut niveau. Ceci est une condition *sine qua non* de contrôle adéquat du fonctionnement de l'organisation et fait partie de l'organisation et de la mise au point d'un système de contrôle interne.

XI.2.12. SUIVI ACTIF DE L'EXTRÉMISME AU SEIN DE LA DÉFENSE PAR LE SGRS

Le Comité permanent R recommande que le SGRS prenne les mesures qui s'imposent pour assurer une participation active aux Local Task Forces (LTF).

Le Comité recommande également que des directives soient établies et qu'une stratégie soit élaborée d'urgence sur le rôle du SGRS dans le cadre du Plan Radicalisme en ce qui concerne le suivi des militaires (de réserve) actifs. Il convient plus particulièrement de définir ce que doit être l'apport précis du SGRS, d'une

part dans le fonctionnement du groupe de travail national et des groupes de travail thématiques, et d'autre part, dans les LTF.

Le Comité permanent R recommande, en outre, que le SGRS déploie des ressources suffisantes pour la détection de l'extrémisme au sein de la Défense. Cela doit être le résultat d'une analyse préalable des ressources nécessaires pour chaque mission/menace.

Par ailleurs, le Comité recommande que le SGRS établisse des directives en rapport avec la consultation et l'alimentation de la Banque de données commune 'Terrorist fighters' (BDC TF) par ses collaborateurs.

XI.2.13. ÉVALUATION DU PLAN STRATÉGIQUE NATIONAL DU RENSEIGNEMENT (PSNR)

Le Comité permanent R invite les ministres de la Justice et de la Défense à procéder à l'évaluation du premier PSNR aux fins de voir renforcer les synergies entre les deux services au vu de ladite évaluation.

XI.2.14. DE MEILLEURES RÈGLES ET CONNAISSANCES SUR L'INTRODUCTION DES ENTITÉS DANS LES BANQUES DE DONNÉES COMMUNES (BDC)

Le Comité permanent R invite la ministre de la Défense à prendre les initiatives nécessaires avec les ministres compétents pour que les textes législatifs et/ou réglementaires établissent dorénavant les règles pour l'éventuelle inscription d'une entité dans la BDC TF ou l'attribution d'un certain niveau à un militaire par l'OCAM.

Le Comité permanent R invite la ministre de la Défense à solliciter les ministres compétents à la mise en œuvre par l'OCAM de recyclages réguliers de ses collaborateurs en la matière.

Le Comité permanent R recommande de revoir le Règlement IF5 qui doit être conforme à la structure et au matériel actuels de la Défense. L'IF5 revisité doit notamment décrire clairement les tâches de l'officier de sécurité et ses prérogatives. Il doit également formaliser les mesures et le contrôle des dépôts de munitions, notamment le rôle et les missions du SGRS.

XI.2.15. L'ÉCHANGE D'INFORMATIONS ENTRE SERVICES DE RENSEIGNEMENT CONCERNANT LE PERSONNEL DE LA DÉFENSE

Le Comité permanent R recommande que la VSSE informe systématiquement le SGRS lorsqu'elle possède des informations concernant le personnel (civil ou militaire) de la Défense. D'autre part, il apparaît nécessaire de voir les deux services conclure un accord de collaboration en matière de suivi du personnel de la Défense.

XI.2.16. RESPECT DES ACCORDS HUMINT[393]

Le Comité permanent R insiste sur le respect des accords conclus entre les services de renseignement en ce qui concerne le HUMINT, tel que repris dans le Plan Stratégique National du Renseignement.

XI.2.17. RESPECT DU TRANSFERT D'INFORMATIONS À L'OCAM

Le Comité permanent R recommande, comme le prévoit la L.OCAM, que les services de renseignement fournissent à l'OCAM, systématiquement et dans le respect des délais légaux, toute information pertinente pour l'analyse et l'évaluation de la menace.

XI.2.18. UNE POLITIQUE DE RECRUTEMENT FLEXIBLE ET PROACTIVE POUR LES SERVICES DE RENSEIGNEMENT

Le Comité permanent R recommande que les services de renseignement aient la possibilité de mener une politique de recrutement flexible et proactive. Ceci nécessite une meilleure collaboration avec le SELOR, mais également un renforcement du personnel nécessaire pour gérer le flux entrant de personnel civil prévu dans les années à venir.

---

393 Les recommandations reprises aux points XI.2.17 à XI.2.31. sont issues de l'enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings (Chapitre I.9.). Un niveau de priorité élevé a été attribué à ces recommandations.

XI.2.19. UN ENVIRONNEMENT DIGITAL DE QUALITÉ

Pour conserver le personnel, il faut par ailleurs que le SGRS dispose d'un environnement digital à la hauteur de ses obligations et missions. Le dernier rapport du Comité en la matière a montré l'insuffisance de l'infrastructure globale IT pour un service de cette importance.

XI.2.20. UNE MÉTHOLOGIE UNIFORME EN MATIÈRE D'ÉVALUATION DE LA MENACE DANS LE DOMAINE DU RENSEIGNEMENT

Le Comité permanent R recommande, afin d'améliorer la communication entre les différents partenaires du secteur du renseignement (VSSE et OCAM en particulier) que le SGRS s'aligne autant que possible sur la (ou les) méthodologie(s) déjà éprouvée(s) par ses partenaires, de manière telle qu'une même menace reçoive la même attention au sein de la communauté du renseignement.

Cette méthodologie doit comprendre une mise à jour des fiches individuelles à réaliser quant aux mesures de collecte de données à prévoir et quant aux actions à entreprendre auprès de l'objet de la menace.

L'ensemble de la 'watchlist' doit faire l'objet d'une réévaluation périodique au terme de laquelle les niveaux de menaces sont (ré)évalués et les menaces identifiées (dans les fiches individuelles) maintenues, revues à la hausse ou à la baisse, voire complètement écartées du système d'information lorsque l'analyse menée révèle que l'attention du SGRS n'est plus (ou pas) requise.

Le Comité permanent R recommande également que le principe de la 'watchlist' soit systématiquement 'implémenté' pour toutes les menaces de la compétence du SGRS, à savoir également celles qui ne nécessitent qu'un niveau minimal de suivi (suivi passif) mais en nécessite néanmoins un. Dès lors que la 'watchlist' comporte des niveaux de menace et les mesures de suivi à y réserver, il n'apparaît pas justifié de maintenir deux documentations distinctes : elle doit pouvoir donner une vision globale de la menace.

XI.2.21. L'IMPORTANCE DE DIVERS RÈGLEMENTS

Le Comité permanent R invite la ministre de la Défense à rappeler au ministre de la Justice la COL 8/2014, actualisée en janvier 2018, et à insister sur le respect systématique de cette circulaire.

Le Comité permanent R recommande d'harmoniser, de (ré)écrire et de centraliser les règles (SOP).

Le Comité permanent R recommande que le SGRS, et par extension la Défense, s'inscrivent dans le Plan R et collaborent dans un état d'esprit constructif.

XI.2.22. AUTORITÉ DISCIPLINAIRE SUR LE PERSONNEL CIVIL DE LA DÉFENSE

Le Comité permanent R recommande une nouvelle fois de remédier à la situation actuelle, le Chef du SGRS ne disposant pas de l'autorité disciplinaire sur le personnel civil du SGRS. Il faut absolument établir une unité de Commandement et non deux chaînes parallèles (une civile, une militaire), comme c'est le cas actuellement.

XI.2.23. UTILISATION DES MÉTHODES DE RECUEIL DE DONNÉES

Le Comité permanent R recommande d'utiliser au maximum les possibilités (Méthodes de recueil de données (MRD), HUMINT, etc.) prévues par les lois pour recueillir des informations, en collaboration avec la VSSE aux fins d'optimalisation.

XI.2.24. RECRUTEMENT DE JURISTES

Le Comité permanent R recommande de recruter davantage de juristes pour assurer une fonction juridico-opérationnelle en appui aux collaborateurs chargés de la collecte et des analystes.

XI.2.25. INVESTIR DANS LE MANAGEMENT

Le Comité permanent R recommande que le SGRS investisse dans une stratégie de 'knowledge management'.

Le Comité permanent R recommande de réformer le *Steering Committee* pour en faire un comité de direction à part entière et efficace, qui doit recevoir les moyens nécessaires pour se concentrer sur sa tâche de coordination et de synchronisation de toutes les activités de renseignement. Il devrait se voir supprimer la gestion des projets à moyen et long terme ainsi que son intervention dans la logistique de base. D'autres entités sont prévues au SGRS pour effectuer ces tâches, mais elles ne sont pas correctement effectuées par manque de personnel.

XI.2.26. CLARIFICATION DES MISSIONS DE COUNTERINTELLIGENCE AU SEIN DU SGRS

Le Comité permanent R recommande que le SGRS s'efforce encore de préciser les missions en matière de 'Counterintelligence' et de les faire connaître à tous les départements des Forces armées.

XI.2.27. FONCTIONNEMENT DES OFFICIERS DE SÉCURITÉ AU SEIN DU SGRS

Le Comité permanent R recommande que le SGRS conscientise davantage les officiers de sécurité (S2) sur l'ensemble des problèmes de sécurité qui peuvent se poser, les responsabilise et les exhorte à assurer une collaboration plus proactive entre les unités et le SGRS. Le SGRS doit quant à lui établir une relation de confiance avec les différents officiers de sécurité.

XI.2.28. IDENTIFICATION D'INDICATEURS DE RADICALISATION PAR LE SGRS

Le Comité permanent R recommande qu'en matière de détection de la radicalisation, le SGRS, épaulé par la Défense, donne des instructions précises afin d'identifier des indicateurs clairs de radicalisation.

XI.2.29. VISIBILITÉ DES ENTITÉS RESPECTIVES À SUIVRE PAR LA VSSE ET LE SGRS

Le Comité permanent R recommande de chercher une solution de type informatique (hit/no hit) pour permettre aux deux services de renseignement de prendre connaissance de leurs entités respectives à suivre, tout en respectant les finalités et le secret des sources propres à chacun des services.

XI.2.30. LES MOYENS POUR LA LUTTE CONTRE L'EXTRÉMISME

Le Comité permanent R recommande que le SGRS soit doté de moyens suffisants pour être en mesure de détecter l'extrémisme au sein de la Défense. Ceci doit

résulter d'une analyse préalable des moyens requis pour les différentes missions/ menaces.

XI.2.31. ACTUALISATION DE DIRECTIVES EXISTANTES[394]

Les directives du Comité ministériel du renseignement et de la sécurité portant sur toutes sortes de règles de sécurité (portée des enquêtes de sécurité, règles de classification, conservation des pièces classifiées, infosec, missions des officiers de sécurité) devraient être actualisées. Ces directives en question datent toutes de 2001.

Le Comité permanent R invite la ministre de la Défense à envisager, avec ses collègues compétents, d'établir une directive commune pour définir les critères légaux (Loi du 11 décembre 1998).

XI.2.32. CUMUL AU SEIN DE LA DÉFENSE

Le Comité permanent R recommande que la Défense puisse s'interroger sur la possibilité offerte aux militaires d'exercer une profession complémentaire dans le domaine de la 'sécurité privée' et sur la conformité de celle-ci avec la dignité de la fonction militaire.

XI.2.33. LE FONCTIONNEMENT DES BANQUE DE DONNÉES COMMUNES AU SEIN DU SGRS

Le Comité permanent R recommande que le SGRS informe son personnel de l'existence de la BDC TF et les sensibilise à son intérêt et à son utilisation. Il convient également d'établir des directives en rapport avec la consultation et l'alimentation de la BDC TF par le SGRS. De plus, un scénario doit être établi pour l'éventuelle inscription d'un militaire dans la BDC TF ou l'attribution d'un certain niveau de menace à un militaire par l'OCAM.

Le Comité permanent R recommande que les services de renseignement désignent des responsables pour consulter systématiquement et quotidiennement la BDC TF et, si nécessaire, partagent les informations avec la ligne hiérarchique jusqu'au plus haut niveau. En outre, le SGRS doit de toute urgence intégrer dans son fonctionnement la finalité (consultation, alimentation, etc.) des banques de

[394] Les recommandations reprises aux points XI.2.32 à XI.2.36. sont issues de l'enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings (Chapitre I.9.). Un niveau de priorité 'urgence moyenne' a été attribué à ces recommandations.

données communes. Par ailleurs, le SGRS doit systématiquement mettre à jour la liste des utilisateurs de la BDC TF.

XI.2.34. NOTIFICATION ET SUIVI DES INCIDENTS DE SÉCURITÉ AU SEIN DU SGRS

Le Comité permanent R recommande que le SGRS établisse un rapport détaillé de tout incident de sécurité. Ce rapport doit reprendre un examen et une analyse de toutes les dimensions (pas seulement techniques, mais aussi comportementales), et a fortiori si un des intéressés détient une habilitation de sécurité. Ce rapport doit être transmis aux autorités de sécurité compétentes, éventuellement avec une proposition de décision.

XI.2.35. COLLABORATION ENTRE LES BUREAUX DE SÉCURITÉ DU SGRS ET DE LA VSSE

Le Comité permanent R recommande que le bureau de sécurité de la VSSE et la Direction S du SGRS collaborent de manière plus étroite et plus formelle, en concluant un protocole d'accord.

XI.2.36. UTILISATION COHÉRENTE DES NIVEAUX DE LA MENACE ET COMMUNICATION DES ÉVALUATIONS PAR L'OCAM[395]

Lors de l'attribution d'un niveau de menace (1, 2, 3 ou 4), une catégorie pour le suivi (A, B ou C) est également accordée lors de l'enregistrement dans la BDC. Les deux paramètres sont indépendants. Les Comités permanents R et P recommandent une amélioration de la cohérence et de l'harmonisation entre le niveau de menace d'une part et la catégorie de suivi d'autre part.

En ce qui concerne le mode de communication et les destinataires des analyses de la menace de l'OCAM, il y a une différence selon qu'il s'agit d'une évaluation de la menace ponctuelle visant des personnes, des groupements ou des événements ou d'une évaluation de la menace individuelle par une personne. Les Comités permanents R et P recommandent, au niveau de la communication de l'évaluation de la menace par une personne, en plus de l'enregistrement dans la BDC, d'également communiquer cette analyse de la menace aux services intéressés

395 Voir Chapitre 'I.10. Le rôle de l'OCAM dans le suivi du militaire Jürgen Conings'. Pour rappel, cette enquête a été réalisée conjointement avec le Comité permanent P.

qui reçoivent les évaluations de la menace contre des personnes conformément à la L. OCAM.

En dépit du pragmatisme dont l'OCAM fait preuve lors de l'application de la Circulaire du ministre de l'Intérieur et du ministre de la Justice concernant l'échange d'informations à propos de Terrorist Fighters et de Propagandistes de haine et de leur suivi, les Comités permanents R et P ont relevé l'importance d'adapter la Circulaire aux nouvelles catégories ajoutées par l'arrêté de modification du 20/12/2019 à la BDC, à savoir les Extrémistes Potentiellement Violents (E.P.V.) et les Personnes Condamnées pour Terrorisme (P.C.T.).

En ligne avec la recommandation précédente, il pourrait être utile, dans le cadre d'une adaptation de la Circulaire des ministres de l'Intérieur et de la Justice concernant l'échange d'informations à propos de Terrorist Fighters et de Propagandistes de haine et de leur suivi, d'évaluer les possibilités d'étendre les mesures existantes de réduction de la menace et de les préciser pour les catégories existantes et nouvelles.

XI.2.37. COMMUNICATION ÉCRITE EN CAS D'APPLICATION DE L'ARTICLE 19 L.R&S[396]

L'article 19 L.R&S ne précise pas de quelle manière les renseignements doivent être communiqués aux ministres concernés et autres. Le Comité permanent R estime que la communication doit se faire par écrit, et ce pour des raisons de sécurité juridique, excepté en cas d'extrême urgence. L'objectif est d'éviter des discussions par la suite et de permettre un contrôle parlementaire (voire juridique). Le Comité recommande de mettre en œuvre sans délai le principe d'une communication écrite systématique.

XI.2.38. LE TRAITEMENT D'INFORMATIONS CLASSIFIÉES PAR DES TIERS[397]

Les destinataires d'information classifiées doivent être prudents avec de telles notes et être conscients des dommages qu'ils pourraient causer aux personnes qui font l'objet de ces notes ainsi qu'au bon fonctionnement des services de renseignement et de sécurité.

Le Comité permanent R invite la VSSE et l'Autorité nationale de sécurité (ANS) à prendre les initiatives nécessaires, dans un délai de six mois, afin de sensibiliser les destinataires et de rappeler les tâches qui incombent aux officiers de sécurité.

---

396 Voir Chapitre 'I.11. Le suivi d'un commissaire de gouvernement par la VSSE'.

397 *Ibid.*

XI.2.39. DES SCREENINGS DE SÉCURITÉ POUR DES FONCTIONS DE CONFIANCE[398]

Le Comité permanent R estime que l'exercice de certaines « fonctions publiques » requiert la vérification préalable de l'intégrité, de la loyauté et de la discrétion, comme l'exige la législation en vigueur dans certains pays européens.

Cette vérification devrait, selon le Comité, notamment être réalisée pour les candidats à la fonction de commissaire du gouvernement mais aussi à d'autres fonctions publiques comme celle d'aumônier, ou d'autres fonctions clés au niveau fédéral, régional et communautaire.

Par conséquent, le Comité permanent R invite le gouvernement à prendre les initiatives législatives pour la fin avril 2022 avec les ministres fédéraux compétents. Le ministre de la Défense est invité à préciser si des fonctions clés au sein de la Défense doivent être intégrée à ces initiatives. Dans le cas contraire, le ministre est invité à prendre les initiatives législatives parallèles nécessaires pour établir le cadre légal des vérifications pour les fonctions l'exigeant au sein de la Défense. Enfin, à l'initiative du ministre de la Justice, la question d'une vérification préalable de fonctions clés aux autres niveaux de pouvoir devrait également être mise à l'agenda d'une réunion du Comité de concertation.

XI.2.40. INDICATION DES DESTINATAIRES SUR LES NOTES SORTANTES[399]

Afin de limiter les fuites, le Comité permanent R recommande que la VSSE mentionne, dans les notes qu'elle rédige, l'ensemble des destinataires de celles-ci et 'individualise' lesdites notes lors de leur envoi.

Le Comité permanent R recommande qu'en règle générale les notes de la VSSE validées en Comité de direction soient transmises sans délai aux destinataires repris dans ces notes.

---

398 Voir Chapitres 'I.11. Le suivi d'un commissaire de gouvernement par la VSSE' & 'I.12. Le suivi des Frères musulmans et l'évaluation de la menace éventuelle que ceux-ci constituent en Belgique'.

399 Voir Chapitre 'I.11. Le suivi d'un commissaire de gouvernement par la VSSE.'

XI.2.41. COMMUNIQUER LES BESOINS DU CONSEIL NATIONAL DE SÉCURITÉ AUX SERVICES DE RENSEIGNEMENT[400]

Le Comité permanent R invite le Conseil national de sécurité (CNS) à préciser aux services de renseignement le type et la nature des notes qu'il souhaite recevoir ainsi que les délais d'envoi.

XI.2.42. COLLABORATION DANS LE CADRE DE LA PROBLÉMATIQUE DES FRÈRES MUSULMANS[401]

Le Comité permanent R est d'avis qu'il appartient aux ministres de la Justice et de la Défense de renforcer avec leurs collègues de l'Intérieur la coopération entre les services de renseignement et leurs partenaires (la Police fédérale, l'OCAM, etc.) et de déterminer, avec les services le cadre de coopération adéquat. Un plan d'action sur la problématique des Frères musulmans devra être mis en œuvre en 2022. Il aura :

- à définir de manière commune :
  - Le phénomène et ses éléments constitutifs ;
  - Le niveau de la menace constituée par celui-ci ;
  - Une stratégie de suivi du phénomène (avec une éventuelle répartition des tâches dans le respect du cadre légal)[402] tenant compte des moyens dont disposent les services ;
  - Une stratégie de sensibilisation des autorités et administrations (avec une répartition des compétences dans le respect du cadre légal).
- à établir une liste actualisée des associations liées aux Frères musulmans, des membres et sympathisants du mouvement ;
- à s'assurer que la capacité des effectifs est garantie pour en assurer le suivi adéquat.

---

400 *Ibid.*

401 Les recommandations reprises aux points XI.2.43 à XI.2.46. sont issues de l'enquête de contrôle 'Une attention renouvelée pour les Frères musulmans' (Chapitre I.12.).

402 Cet exercice a déjà été réalisé pour ce qui concerne le SGRS et la VSSE, et acté dans les plans stratégiques (voir *supra*).

XI.2.43. ANALYSE DES MOYENS DU SGRS DANS LE CADRE DE LA PROBLÉMATIQUE DES FRÈRES MUSULMANS

Le Comité permanent R recommande au SGRS de procéder en 2022 à une analyse pour déterminer si les moyens qu'il déploie pour le suivi des Frères musulmans sont suffisants au regard de la probabilité estimée du risque de tentative d'influence des Frères musulmans à l'égard de la Défense, et tenant compte de la priorité accordée au suivi du phénomène par le service. Dans le cas contraire, il appartient au SGRS d'inviter la ministre de la Défense à établir un plan de recrutement adéquat.

XI.2.44. SENSIBILISATION GÉNÉRALE DANS LE CADRE DE LA PROBLÉMATIQUE DES FRÈRES MUSULMANS

La Comité permanent R salue l'ambition de la VSSE de réaliser une brochure sur les Frères musulmans pour une diffusion large dans un but de sensibilisation et recommande à la VSSE de diffuser celle-ci au plus tard à la fin de l'année 2022.

XI.2.45. SENSIBILISATION DES OFFICIERS DE SÉCURITÉ DE LA DÉFENSE DANS LE CADRE DE LA PROBLÉMATIQUE DES FRÈRES MUSULMANS

Le Comité permanent R invite le SGRS à organiser des briefings internes pour les officiers de sécurité désignés afin de les sensibiliser à la problématique, et augmenter leur capacité de détection d'une menace concrète pour la Défense.

XI.2.46. L'ICT DANS LE PROCESSUS DU RENSEIGNEMENT AU SEIN DE LA DIRECTION CYBER DU SGRS[403]

Le Comité permanent R recommande de prendre en compte les points suivants en vue de garantir une efficacité optimale du service, et ce afin que celui-ci puisse remplir ses objectifs stratégiques :
- Effectuer les engagements nécessaires correspondants au plan de personnel, tel qu'il a été présenté au Comité permanent R ;
- Prendre des mesures complémentaires (*no-break*, UPS complémentaire, monitoring) afin de pallier les problèmes d'infrastructure électrique du quartier ;

[403] Voir Chapitre 'I.13. Les technologies de l'information et de la communication dans le processus de renseignement au sein de la Direction Cyber du SGRS et au sein de la VSSE'.

– Augmenter les ressources hardwares lorsque cela serait nécessaire afin de garantir une meilleure qualité de service rendu aux utilisateurs ;
– Porter une grande attention aux contrats avec des firmes externes, par exemple en envisageant des logiciels '*on premises*' (sur infrastructure propre).

XI.3. RECOMMANDATION RELATIVE À L'EFFICACITÉ DU CONTRÔLE

XI.3.1. SIGNALEMENT PAR LE SGRS DU SUIVI DES MANDATAIRES POLITIQUES[404]

Le Comité permanent R recommande au SGRS de lui remettre tous les trois mois un aperçu de tous les documents dans lesquels des mandataires politiques sont mentionnés, le cas échéant, avec une absence de « hit » si aucune mention de ce genre n'a été faite.

[404] Voir Chapitre 'I.8. Enquête de contrôle sur le suivi des mandataires politiques'.

ANNEXES

ANNEXE A
APERÇU DES PRINCIPALES RÉGLEMENTATIONS RELATIVES AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2021 AU 31 DÉCEMBRE 2021)

Loi du 27 juin 2021 contenant le troisième ajustement du budget général des dépenses pour l'année budgétaire 2021, *M.B.* 9 juillet 2021

Loi du 14 août 2021 modifiant la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace et visant à élargir les conditions de nomination des greffiers du Comité R et du Comité P, *M.B.* 8 décembre 2021

Loi du 23 décembre 2021 contenant le budget général des dépenses pour l'année budgétaire 2022, *M.B.* 29 décembre 2021

A.R. 30 septembre 2021 fixant la liste des bénéficiaires des actions menées par le Service public fédéral Stratégique et Appui dans le cadre de sa mission de développement d'initiatives culturelles, promotionnelles, divertissantes, formatrices et sportives, *M.B.* 4 novembre 2021

Directive commune des ministres de la Justice et de l'Intérieur relative à la détermination des modalités de communication des données à caractère personnel et informations traitées dans le cadre de leurs missions de police administrative et judiciaire, telles que visées aux articles 14 et 15 de la loi sur la fonction de police, par les services de police et à l'accès direct et l'interrogation directe de la BNG, *M.B.* 2 février 2021

Appel aux candidats pour la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité, *M.B.* 12 février 2021

Par arrêté ministériel du 3 février 2021, le mandat de directeur d'encadrement de la Sûreté de l'État de Monsieur Hugues Brulin, est renouvelé pour une durée de 5 ans, à partir du 1er septembre 2020, *M.B.* 16 février 2021

Avis prescrit par l'article 3*quater* de l'arrêté du Régent du 23 août 1948 déterminant la procédure devant la section du contentieux administratif du Conseil d'État l'association sans but lucratif Syndicat de la Police Belge, "Sypol.be", a demandé l'annulation de l'arrêté royal du 24 septembre 2020 'modifiant l'arrêté royal du 13 décembre 2006 portant le statut des agents des services extérieurs de la Sûreté de l'État', *M.B.* 16 février 2021

Directeur de l'Organe de coordination pour l'analyse de la menace, fin de la désignation, *M.B.* 24 février 2021

Directeur de l'Organe de coordination pour l'analyse de la menace, désignation ad interim, *M.B.* 24 février 2021

Comité permanent de contrôle des services de renseignements et de sécurité, poste vacant pour un attaché francophone (m/f/x) de niveau universitaire, *M.B.* 5 mars 2021

Recrutement, par détachement, et constitution d'une réserve de recrutement de commissaires-auditeurs francophones (m/f/x), dotés de connaissances particulières en gestion des enquêtes judiciaires et en gestion de l'information (Intelligence-led Policing), pour le Service d'Enquêtes du Comité permanent R, *M.B.* 18 mars 2021

Appel aux candidats pour la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité, *M.B.* 2 avril 2021

Nomination du greffier du Comité permanent de contrôle des services de renseignement (Comité R), *M.B.* 19 juillet 2021

Cour Constitutionnelle : extrait de l'arrêt n° 64/2021 du 22 avril 2021, n° du rôle : 7416, en cause : la question préjudicielle relative à l'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, posée par le Comité permanent de contrôle des services de renseignement et de sécurité, *M.B.* 20 septembre 2021

Recrutement, par détachement, et constitution d'une réserve de recrutement de commissaires-auditeurs francophones (m/f/x), dotés de connaissances particulières en ICT/Data, pour le Service d'Enquêtes du Comité permanent R, *M.B.* 1er octobre 2021

Cour Constitutionnelle : extrait de l'arrêt n° 107/2021 du 15 juillet 2021, n° du rôle : 7261, en cause : le recours en annulation de la loi du 23 mars 2019 'concernant l'organisation des services pénitentiaires et le statut du personnel pénitentiaire', introduit par Michel Jacobs, *M.B.* 6 octobre 2021

Appel à candidats pour le mandat de second membre suppléant néerlandophone du Comité permanent de contrôle des services de renseignement (Comité R), *M.B.* 25 novembre 2021

Recrutement, par détachement, et constitution d'une réserve de recrutement de commissaires-auditeurs francophones (m/f/x), dotés de connaissances particulières en ICT/Data, pour le Service d'Enquêtes du Comité permanent R, *M.B.* 23 décembre 2021

Sélection comparatives, épreuves préalables des sélections comparatives et résultats des sélections comparatives de :

- HR Business Partners pour le service de renseignement militaire (m/f/x) (niveau A1), néerlandophones, pour le Ministère de la Défense, n° de sélection : ANG21132, *M.B.* 17 mai 2021
- HR Business Partners pour le service de renseignement militaire (m/f/x) (niveau A1), francophones, pour le Ministère de la Défense, n° de sélection : ANG21132, *M.B.* 17 mai 2021
- Data Officers (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, n° de sélection : AFG21100, *M.B.* 1er juin 2021
- Data Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21130, *M.B.* 1er juin 2021
- Technical Officers (m/f/x) (niveau B), francophones, pour la Sûreté de l'État. - n° de sélection : AFG21102, *M.B.* 1er juin 2021
- Technical Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État. - n° de sélection : ANG21134, *M.B.* 1er juin 2021
- Administrateurs système Windows/Linux (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, n° de sélection : AFG21119, *M.B.* 13 juillet 2021
- Gestionnaires de réseaux (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21153, *M.B.* 13 juillet 2021
- Collaborateurs Imagery Intelligence pour le Service général du Renseignement et de Sécurité (SGRS) (m/f/x) (niveau B), néerlandophones, pour le Ministère de la Défense, n° de sélection : ANG21216, *M.B.* 16 juillet 2021
- Documentalistes renseignement et sécurité (m/f/x) (niveau B) néerlandophones, pour le Ministère de la Défense, n° de sélection : ANG21218, *M.B.* 26 juillet 2021

- Spécialistes Query & Reporting (m/f/x) (niveau A1), francophones, pour le Ministère de la Défense, n° de sélection : AFG21134, *M.B.* 6 août 2021
- Attachés analyste habilitation de sécurité (m/f/x) (niveau A), francophones, pour le Ministère de la Défense, n° de sélection : AFG21135, *M.B.* 6 août 2021
- Chercheur en cyber défense A2 (m/f/x) (niveau A2), francophones, pour le Ministère de la Défense, n° de sélection : AFG21156, *M.B.* 16 août 2021
- Inspecteurs francophones pour les services extérieurs (m/f/x) (niveau B) de la Sûreté de l'État, n° de sélection : AFG21149, *M.B.* 29 septembre 2021
- Inspecteurs néerlandophones pour les services extérieurs (m/f/x) (niveau B) de la Sûreté de l'État, n° de sélection : AFG21212, *M.B.* 29 septembre 2021
- Finance Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21303, *M.B.* 30 septembre 2021
- Technical Officers (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, n° de sélection : AFG21102, *M.B.* 26 octobre 2021
- Administrateurs système Windows/Linux (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, n° de sélection : AFG21119, *M.B.* 26 octobre 2021
- Technical Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21134, *M.B.* 26 octobre 2021
- Gestionnaires de réseaux(m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21153, *M.B.* 26 octobre 2021
- Attachés analystes habilitation de sécurité (m/f/x) (niveau A1) francophones pour le Ministère de la Défense, n° de sélection : AFG21135, *M.B.* 17 novembre 2021
- Néerlandophones d'accession au niveau B (épreuve particulière) pour la Sûreté de l'État, n^{os} de sélection : BNG21341 et BNG21342, *M.B.* 8 décembre 2021
- francophones d'accession au niveau B (épreuve particulière) pour la Sûreté de l'État, n^{os} de sélection : BFG21188 et BFG21189, *M.B.* 8 décembre 2021
- Data Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21130, *M.B.* 16 décembre 2021
- Data Officers (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, n° de sélection : AFG21100, *M.B.* 16 décembre 2021
- Finance Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21303, *M.B.* 27 décembre 2021
- Inspecteurs pour les services extérieurs (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, n° de sélection : AFG21149, *M.B.* 30 décembre 2021
- Inspecteurs néerlandophones pour les services extérieurs (m/f/x) (niveau B) de la Sûreté de l'État, n° de sélection : ANG21212, *M.B.* 30 décembre 2021

ANNEXE B
APERÇU DES PRINCIPALES PROPOSITIONS DE LOIS, DES PROJETS DE LOIS, DES RÉSOLUTIONS, MOTIONS D'ORDRE ET DES DÉBATS PARLEMENTAIRES RELATIFS AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2021 AU 31 DÉCEMBRE 2021)

Sénat

Rapport d'information concernant la nécessaire collaboration entre l'autorité fédérale et les Communautés en matière de lutte contre les infox (fake news) de S. D'Hose, E. Ampe, R. Daems, W.-F. Schiltz, C. Van Cauter, F. Ahallouch, L. Gahouchi, G.-L. Bouchez, Ph. Dodrimont, V. Durenne, S. Laruelle, A. Miesen, G. Van Goidsenhoven, J.-P. Wahl, K. Brouwers, B. Anciaux, K. De Loor, A. Lambrecht, K. Segers, A. Antoine, A.-C. Goffinet, F. Ben Chikha, S. Bex, R. Demeuse, S. Hoessen, F. Masai, J. Pitseys, H. Ryckmans, Ch. Steenwegen et F. Tahar, Doc. 7-110, *Ann. Parl.*, Sénat, 2021-2022, 17 novembre 2021, n° 6-24, p. 5

Cour constitutionnelle, arrêt n° 158/2021, rendu le 18 novembre 2021, en cause le recours en annulation de la loi du 1er septembre 2016 portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, introduit par P. Van Assche et autres (n° du rôle 6672), *Ann. Parl.*, Sénat, 2021-2022, 17 décembre 2021, n° 6-25, p. 43

Chambre des représentants

Commissions, comités d'avis et délégations aux assemblées internationales, Doc. parl., Chambre, 2020-2021, n° 55-8/8

Motions déposées le 17 mars 2021 en réunion publique de commission (Articles 133 à 141 du Règlement de la Chambre) en conclusion de l'interpellation de N. Boukili au Premier ministre sur 'Smals et les marchés publics relatifs à la digitalisation du service public', Doc. parl., Chambre, 2020-2021, n° 55-105/1

Proposition de résolution visant à prévoir dans le plan de retrait de l'Operation Vigilant Guardian (OVG) des moyens équivalents pour les sites présentant un niveau 3 de la menace, Doc. parl., Chambre, 2020-2021, n° 55-1413/2

Proposition de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité en vue de l'instauration d'une obligation de notification active pour certaines méthodes spécifiques de collecte de données, Doc. parl., Chambre, 2020-2021, nº 55-1763/1

Comité permanent de contrôle des services de renseignements et de sécurité – nomination du premier suppléant d'un membre francophone – candidatures introduites, *C.R.I.*, Chambre, 2020-2021, 28 janvier 2021, PLEN 85, p. 38

Proposition de résolution relative à la cyberdéfense et à l'attribution des cyberattaques étatiques, Doc. parl., Chambre, 2020-2021, nº 55-1788/1

Cour des comptes, Cour constitutionnelle, Conseil supérieur de la Justice, Comité permanent de contrôle des services de police, Comité permanent de contrôle des services de renseignements et de sécurité, Médiateurs fédéraux, Autorité de protection des données, Commissions de nomination pour le notariat, Commission BIM, Organe de contrôle de l'information policière, Commission fédérale de déontologie, Conseil central de surveillance pénitentiaire, Institut des droits humains - audit de suivi de la

Cour des comptes - mise en œuvre des recommandations, Doc. parl., Chambre, 2020-2021, nº 55-1924/1

Motion d'ordre déposée par P. De Roover, P. Buysrogge et J. Donné : 'La Chambre des représentants, - considérant que des informations provenant d'un échange de vues au sujet d'une future enquête de contrôle ont été divulguées aux médias par des membres de la commission d'accompagnement parlementaire du Comité P & R; - considérant que la commission d'accompagnement entre dans le champ d'application de l'art. 67 du Règlement de la Chambre et que l'obligation de secret s'applique à l'égard de toutes les informations obtenues dans le cadre des réunions; demande à la présidente de la Chambre de mener une enquête sur les auteurs des infractions, pour ensuite prendre les sanctions appropriées en application de l'art. 67 du Règlement de la Chambre', *C.R.I.*, Chambre, 2020-2021, 27 mai 2021, PLEN 106, p. 26

Communication relative au respect de l'article 67 du Règlement, *C.R.I.*, Chambre, 2020-2021, 27 mai 2021, PLEN 106, p. 27

Projet de loi contenant le premier ajustement du budget des Voies et Moyens de l'année budgétaire 2021 (1920/1-8), projet de loi contenant le troisième ajustement du budget général des dépenses pour l'année budgétaire 2021 (1921/1-27), ajustement des budgets des recettes et des dépenses pour l'année budgétaire 2021. Exposé général (1919/1), *C.R.I.*, Chambre, 2020-2021, 24 juin 2021, PLEN 113, p. 1

Proposition de loi modifiant la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace et visant à élargir les conditions de nomination des greffiers du Comité R et du Comité P (2064/1-3), *C.R.I.*, Chambre, 2020-2021, 8 juillet 2021, PLEN 117, p. 51

Motion déposée par P. De Roover : 'réquisition de la présence du Premier ministre – art. 100 de la Constitution et art. 50 du règlement eu égard aux déclarations du Premier ministre ce lundi en commission de la santé relatives à l'enquête de la Sûreté de l'État sur l'ancienne commissaire du gouvernement pour l'Institut pour l'égalité des femmes et des hommes et à la transmission au cabinet du ministre de la Justice des résultats de celle-ci, *C.R.I.*, Chambre, 2020-2021, 14 juillet 2021, PLEN 119, p. 2

Comité permanent de contrôle des services de renseignements et de sécurité, remplacement du greffier, appel aux candidats, *C.R.I.*, Chambre, 2020-2021, 15 juillet 2021, PLEN 122, p. 44

Proposition de rejet par la commission de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives de la proposition de résolution visant à prévoir dans le plan de retrait de l'Operation Vigilant Guardian (OVG) des moyens équivalents pour les sites présentant un niveau 3 de la menace (1413/1-2), *C.R.I.*, Chambre, 2020-2021, 15 juillet 2021, PLEN 122, p. 62

Proposition de résolution relative à la cyberdéfense et à l'attribution des cyberattaques étatiques, Doc. parl., Chambre, 2020-2021, nº 55-1788/1

Projet de loi modifiant la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace et visant à élargir les conditions de nomination des greffiers du Comité R et du Comité P, Doc. parl., Chambre, 2020-2021, nos 55-2064/1 à 55-2064/4

Projet de loi portant assentiment à l'accord entre le Royaume de Belgique et le Royaume d'Espagne sur l'échange et la protection mutuelle des informations classifiées, fait à Bruxelles le 15 octobre 2015, Doc. parl., Chambre, 2020-2021, nos 55-2074/1 à 55-2074/3

Projet de loi portant assentiment à l'accord entre le Royaume de Belgique et la République de Finlande concernant la protection réciproque des informations classifiées, fait à Helsinki le 20 juillet 2016, Doc. parl., Chambre, 2020-2021, nº 55-2075/1

Projet de loi portant assentiment à l'accord entre le Royaume de Belgique et la République de Chypre sur la protection mutuelle des informations classifiées, fait à Bruxelles le 20 juillet 2015, Doc. parl., Chambre, 2020-2021, nº 55-2085/1

Projet de loi portant assentiment à l'accord entre le Royaume de Belgique et la Hongrie sur l'échange et la protection mutuelle des informations classifiées, fait à Budapest le 21 septembre 2015, Doc. parl., Chambre, 2020-2021, nº 55-2121/1

Actualisation de la vision stratégique, échange de vues avec la ministre de la Défense, Doc. parl., Chambre, 2020-2021, nº 55-2150/1

Proposition de résolution relative à la protection de notre sécurité nationale et de notre indépendance stratégique contre les cyberattaques étrangères grâce à l'établissement d'une liste de fournisseurs à haut risque, Doc. parl., Chambre, 2020-2021, nº 55-2167/1

Cyberattaques menées contre les systèmes IT de l'état et des services publics, Doc. parl., Chambre, 2020-2021, nº 55-2169/1

Comité permanent de contrôle des services de renseignements et de sécurité – nomination du greffier – candidatures introduites, *C.R.I.*, Chambre, 2020-2021, 23 septembre 2021, PLEN 125, p. 27

Comité permanent de contrôle des services de police – nomination du greffier – candidatures introduites, *C.R.I.*, Chambre, 2020-2021, 23 septembre 2021, PLEN 125, p. 29

Affaire Jürgen Conings, Doc. parl., Chambre, 2020-2021, nº 55-2206/1

Rapport d'activités 2020 du Comité permanent de contrôle des services de renseignement et de sécurité, Doc. parl., Chambre, 2021-2022, nº 55-2209/1

Proposition de résolution relative à l'indépendance et au fonctionnement de l'Autorité de protection des données, Doc. parl., Chambre, 2021-2022, nº 55-2246/1

Projet de loi portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques, Doc. parl., Chambre, 2021-2022, nºs 55-2256/1, 55-2256/7 et 55-2256/8

Projet de loi modifiant la loi du 13 juin 2005 relative aux communications électroniques, Doc. parl., Chambre, 2021-2022, nºs 55-2257/1 à 55-2257/4

Les révélations dans la presse concernant le rôle des banques dans le blanchiment de l'argent (FINCEN FILES), Doc. parl., Chambre, 2021-2022, nº 55-2261/1

Projet de loi contenant le budget des Voies et Moyens pour l'année budgétaire 2022, Doc. parl., Chambre, 2021-2022, nº 55-2291/1

Projet de loi contenant le budget général des dépenses pour l'année budgétaire 2022, Doc. parl., Chambre, 2021-2022, nºs 55-2292/1 et 55-2292/6

Justification du budget général des dépenses pour l'année budgétaire 2022, Doc. parl., Chambre, 2021-2022, nºs 55-2293/6 et 55-2293/7

Note de politique générale, Doc. parl., Chambre, 2021-2022, nºs 55-2294/2, 55-2294/8, 55-2294/14, 55-2294/16, 55-2294/17, 55-2294/18 et 55-2294/22

Projet de loi modifiant diverses dispositions relatives au passage au sein de la même catégorie de personnel ou à l'admission dans une autre qualité ou catégorie de personnel du militaire de carrière ou du militaire avec une carrière à durée limitée, Doc. parl., Chambre, 2021-2022, nº 55-2302/1

Comité R – démission du second suppléant du membre néerlandophone, *C.R.I.*, Chambre, 2021-2022, 10 novembre 2021, PLEN 139, p. 68

Cour des comptes, Cour constitutionnelle, Conseil supérieur de la Justice, Comité permanent de contrôle des services de police, Comité permanent de contrôle des services de renseignement et de sécurité, Médiateurs fédéraux, Autorité de protection des données, Commissions de nomination pour le notariat, Commission BIM, Organe de contrôle de l'information policière, Commission fédérale de déontologie, Conseil central de surveillance pénitentiaire, Institut fédéral des droits humains, travaux des groupes de travail dans le cadre du projet de synergie, comptes de l'année budgétaire

2020, ajustements budgétaires de l'année budgétaire 2021, propositions budgétaires pour l'année budgétaire 2022, Doc. parl., Chambre, 2021-2022, nos 55-2368/1 à 55-2368/3, *C.R.I.*, Chambre, 2021-2022, 22 décembre 2021, PLEN 152, p. 27 et *C.R.I.*, Chambre, 2021-2022, 22 décembre 2021, PLEN 154, p. 17

Proposition de loi modifiant la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en vue de soumettre les fournisseurs de services essentiels du service public qui dépendent des réseaux et des systèmes d'information à certaines exigences en matière de sécurité et de notification, Doc. parl., Chambre, 2021-2022, nos 55-2401/1

ANNEXE C
APERÇU DES INTERPELLATIONS, DES DEMANDES D'EXPLICATIONS ET DES QUESTIONS ORALES ET ÉCRITES RELATIVES AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2021 AU 31 DÉCEMBRE 2021)

Sénat

Question écrite de G. D'haeseleer au ministre de la Justice sur les 'personnes condamnées pour terrorisme - nombre - motifs - nationalité' (Sénat, 2020-2021, 3 mars 2021, Q. no 7-1107)

Question écrite de T. Ongena au ministre de la Justice sur la 'Turquie - salafisme - ingérence d'états étrangers - chiffres et tendances' (Sénat, 2020-2021, 5 mars 2021, Q. no 7-1140)

Question écrite de T. Ongena à la ministre de l'Intérieur sur la 'Turquie - salafisme - ingérence d'États étrangers - chiffres et tendances' (Sénat, 2020-2021, 5 mars 2021, Q. no 7-1141)

Question écrite de R. Daems au ministre de la Justice sur les 'médias sociaux - confidentialité en ligne - cryptage - Sûreté de l'État - chiffres et tendances - mesures possibles' (Sénat, 2020-2021, 31 mars 2021, Q. no 7-1154)

Question écrite d'A. Frédéric au ministre de la Justice sur les 'sectes - nouvelles pratiques - lutte - évolution de la législation - moyens institutionnels, financiers et humains - renforcement - crise de la Covid-19 - impact - évaluation' (Sénat, 2020-2021, 28 avril 2021, Q. no 7-1219)

Question écrite de R. Daems au ministre de la Justice sur 'l'écologie - climat - réduction des émissions - objectifs – respect des promesses – 'espionnage vert' - contrôle par les pays tiers et des pays tiers - Sûreté de l'État - participation' (Sénat, 2020-2021, 3 mai 2021, Q. no 7-1227)

Question écrite de T. Ongena au ministre de la Justice sur la 'Turquie - mouvement Gülen - crimes de haine en Belgique - protection policière - incidents - chiffres et tendances - communauté turque - protection - mesures' (Sénat, 2020-2021, 3 mai 2021, Q. no 7-1229)

Question écrite de T. Ongena à la ministre de l'Intérieur sur 'l'extrême droite - sociétés de gardiennage et de sécurité - infiltration - chiffres et tendances' (Sénat, 2020-2021, 21 mai 2021, Q. no 7-1248)

Question écrite de T. Ongena au ministre de la Justice sur 'l'extrême droite - risque d'attentats - concertation - violence - Coronavirus - forums de discussion en ligne (Covid-19)' (Sénat, 2020-2021, 21 mai 2021, Q. no 7-1249)

Question écrite de T. Ongena à la ministre de l'Intérieur sur les 'cyberattaques - cybersécurité - chiffres et tendances - auteurs - acteurs étatiques - vie privée - protection - mesures' (Sénat, 2020-2021, 22 juillet 2021, Q. nº 7-1311)

Question écrite d'A. Miesen à la ministre de la Défense sur les 'Militärdienste - Reform der Nachrichtendienste - Extremismusbekämpfung Services de la Défense - réforme des services de renseignement - lutte contre l'extrémisme' (Sénat, 2020-2021, 24 août 2021, Q. nº 7-1322)

Question écrite d'E. Ampe au ministre de la Justice sur les 'smartphones - acteurs étatiques - vie privée - espionnage - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1385)

Question écrite d'E. Ampe à la ministre de l'Intérieur sur les 'smartphones - acteurs étatiques - vie privée - espionnage - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1386)

Question écrite d'E. Ampe au ministre de la Justice sur les 'smartphones - logiciels de harcèlement - vie privée - espionnage - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1387)

Question écrite d'E. Ampe à la ministre de l'Intérieur sur les 'smartphones - logiciels de harcèlement - vie privée - espionnage - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1388)

Question écrite de R. Daems au ministre de la Justice sur la 'cryptographie - ordinateurs quantiques - vie privée - espionnage - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1391)

Question écrite de R. Daems à la ministre de l'Intérieur sur la 'cryptographie - ordinateurs quantiques - vie privée - espionnage - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1392)

Question écrite de T. Ongena à la ministre de la Défense sur les 'drones - police - espionnage - acteurs étrangers - vie privée - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1395)

Question écrite de T. Ongena à la ministre de l'Intérieur sur les 'drones - police - espionnage - acteurs étrangers - vie privée - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1396)

Chambre des représentants

Question de S. Moutquin au secrétaire d'État à l'Asile et la Migration sur 'la forte croissance du nombre de screenings de sécurité effectuée à la demande de l'OE et du CGRA' (*C.R.I.*, Chambre, 2020-2021, 6 janvier 2021, COM 322, p. 16, Q. nº 11488C)

Interpellation et questions jointes de D. Van Langenhove, K. Metsu et Ph. Pivin au ministre de la Justice sur 'l'avis négatif de la Justice concernant la reprise des activités à la Grande Mosquée de Bruxelles' (*C.R.I.*, Chambre, 2020-2021, 6 janvier 2021, COM 324, p. 1, Q. nºs 58I, 11916C et 12037C)

Question de Th. Francken au ministre de la Justice sur 'l'arrêté de subvention pour l'Exécutif des Musulmans' (*C.R.I.*, Chambre, 2020-2021, 6 janvier 2021, COM 324, p. 36, Q. nº 11948C)

Question de D. Safai au secrétaire d'État à l'Asile et la Migration sur 'le suivi et le contrôle des illégaux radicalisés et des réfugiés reconnus radicalisés en Belgique' (*Q.R.*, Chambre, 2020-2021, 12 janvier 2021, nº 34, p. 151, Q. nº 59)

Question d'E. Burton à la ministre de l'Intérieur sur 'l'arrestation d'un radicalisé devant le commissariat de Bruxelles' (*Q.R.*, Chambre, 2020-2021, 12 janvier 2021, nº 34, p. 394, Q. nº 110)

Question de T. Vandenput à la ministre de l'Intérieur sur 'la mise à jour de la base de données de l'OCAM' (*Q.R.*, Chambre, 2020-2021, 12 janvier 2021, nº 34, p. 408, Q. nº 119)

Question et interpellation jointes de S. De Wit et M. Dillen au ministre de la Justice 'le gardien grièvement blessé à la prison de Gand' (*C.R.I.*, Chambre, 2020-2021, 13 janvier 2021, COM 334, p. 14, Q. nos 12064C et 75I)

Question de K. Metsu à la ministre de l'Intérieur sur 'la lutte contre l'extrémisme violent' (*C.R.I.*, Chambre, 2020-2021, 13 janvier 2021, COM 336, p. 49, Q. nº 11874C)

Question d'E. Samyn à la ministre des Affaires étrangères sur 'le rapport des Nations Unies sur le risque de nouvelles campagnes de terreur de l'EI en Europe' (*Q.R.*, Chambre, 2020-2021, 18 janvier 2021, nº 35, p. 91, Q. nº 117)

Question de J. Pillen à la ministre de la Défense sur le 'port de l'uniforme par des militaires' (*Q.R.*, Chambre, 2020-2021, 18 janvier 2021, nº 35, p. 297, Q. nº 83)

Question de K. Jadin à la ministre de l'Intérieur sur 'les interpellations pour menace de personnalités publiques' (*Q.R.*, Chambre, 2020-2021, 18 janvier 2021, nº 35, p. 405, Q. nº 171)

Débat d'actualité et questions jointes de B. Segers, H. Rigot, S. Moutquin, T. Vandenput et G. Daems au secrétaire d'État à l'Asile et la Migration sur 'l'affaire Kucam' (*C.R.I.*, Chambre, 2020-2021, 19 janvier 2021, COM 337, p. 1, Q. nos 12673C, 12674C, 12721C, 12723C, 12735C et 12756C)

Question de Th. Francken au secrétaire d'État à l'Asile et la Migration sur 'le renvoi des extrémistes' (*C.R.I.*, Chambre, 2020-2021, 19 janvier 2021, COM 337, p. 18, Q. nº 12073C)

Question de K. Jadin au ministre de la Justice sur 'l'extrême droite en Belgique' (*C.R.I.*, Chambre, 2020-2021, 21 janvier 2021, PLEN 084, p. 42, Q. nº 1286P)

Question de J. Pillen à la ministre de la Défense sur 'les intrusions sur les domaines militaires' (*Q.R.*, Chambre, 2020-2021, 27 janvier 2021, nº 36, p. 349, Q. nº 80)

Question d'A. Ponthier à la ministre de la Défense sur 'la fraude téléphonique depuis la Syrie' (*Q.R.*, Chambre, 2020-2021, 27 janvier 2021, nº 36, p. 352, Q. nº 92)

Question de J. Pillen à la ministre de la Défense sur les 'appels téléphoniques suspects' (*Q.R.*, Chambre, 2020-2021, 27 janvier 2021, nº 36, p. 356, Q. nº 98)

Questions jointes de B. Moyaers, P. Pivin, S. Matheï et K. Van Vaerenbergh au ministre de la Justice sur 'les appels aux émeutes en Belgique diffusés par les médias sociaux' (*C.R.I.*, Chambre, 2020-2021, 28 janvier 2021, PLEN 85, p. 2, Q. nos 1303P, 1311P,1312P et 1315P)

Question de M. Freilich à la ministre de la Fonction publique sur 'la campagne d'intimidation de Huawei contre le gouvernement belge' (*C.R.I.*, Chambre, 2020-2021, 24 février 2021, COM 387, p. 6, Q. nº 12479C)

Question de Th. Francken, D. Ducarme et G. Dallemagne au ministre de la Justice sur 'le CCIF en Belgique' (*C.R.I.*, Chambre, 2020-2021, 24 février 2021, COM 389, p. 17, Q. nos 14172C, 14331C et 14455C)

Question de L. Dierick au ministre de la Justice sur 'les délais de paiement au SPF Justice' (*Q.R.*, Chambre, 2020-2021, 4 mars 2021, nº 41, p. 167, Q. nº 289)

Question de J.-M. Delizée au ministre de la Justice sur 'la déclassification des archives dites africaines' (*Q.R.*, Chambre, 2020-2021, 4 mars 2021, nº 41, p. 178, Q. nº 369)

Débat d'actualité et questions jointes d'H. Rigot, B. Segers, P. De Roover, S. Moutquin, G. Daems et E. Platteau au secrétaire d'État à l'Asile et la Migration sur 'les nouveaux soupçons de trafic de visas humanitaires' (*C.R.I.*, Chambre, 2020-2021, 9 mars 2021, COM 397, p. 1, Q. nos 14898C, 14920C, 15041C, 15045C, 15067C et 15086C)

Débat d'actualité et questions jointes de Th. Francken, J. Pillen, A. Ponthier, H. Bayet, G. Defossé et K. Verduyckt à la ministre de la Défense sur 'l'amélioration des conditions des

militaires' (*C.R.I.*, Chambre, 2020-2021, 10 mars 2021, COM 402, p. 1, Q. nos 12466C, 13889C, 14028C, 14251C, 14265C, 15097C, 15109C et 15144C)

Question d'E. Van Hoof à la ministre des Affaires étrangères sur 'les déclarations du diplomate iranien traduit en justice' (*Q.R.*, Chambre, 2020-2021, 11 mars 2021, no 42, p. 115, Q. no 60)

Question de W. Vermeersch au ministre des Finances sur la 'douane - la préoccupation croissante suscitée par les scanneurs chinois' (*Q.R.*, Chambre, 2020-2021, 11 mars 2021, no 42, p. 205, Q. no 230)

Question de M. Freilich au ministre des Finances sur 'Nuctech - scanners chinois' (*Q.R.*, Chambre, 2020-2021, 11 mars 2021, no 42, p. 208, Q. no 231)

Question de K. Metsu au ministre de la Justice sur les 'perquisitions dans le cadre de l'enquête sur le financement des groupes terroristes' (*Q.R.*, Chambre, 2020-2021, 11 mars 2021, no 42, p. 288, Q. no 368)

Question d'A. Ponthier à la ministre de la Défense sur 'la coopération entre des universités belges et les Seven Sons of National Defence en Chine' (*Q.R.*, Chambre, 2020-2021, 11 mars 2021, no 42, p. 304, Q. no 124)

Questions jointes de B. Segers, F. Demon et K. Gabriëls au ministre de la Justice sur 'l'opération Sky' (*C.R.I.*, Chambre, 2020-2021, 11 mars 2021, PLEN 91, p. 24, Q. nos 1428P, 1431P et 1430P)

Questions jointes de K. Aouasti, N. Gilson, N. Boukili, G. Dallemagne et G. Vanden Burre au ministre de la Digitalisation sur 'le respect de la vie privée et le projet 'Putting data at the center" (*C.R.I.*, Chambre, 2020-2021, 11 mars 2021, PLEN 91, p. 35, Q. nos 1427P, 1435P, 1438P, 1445P et 1449P)

Question de S. Van Hecke au ministre de la Justice sur 'le suivi des organisations sectaires dans le cadre de la crise du coronavirus' (*Q.R.*, Chambre, 2020-2021, 17 mars 2021, no 43, p. 218, Q. no 381)

Question de S. Goethals à la ministre de l'Intérieur sur les 'organes relevant de vos compétences' (*Q.R.*, Chambre, 2020-2021, 17 mars 2021, no 43, p. 269, Q. no 313)

Question de Ph. Pivin à la ministre de l'Intérieur sur les 'mesures de protection des enseignants - menace radicalisme et terrorisme' (*Q.R.*, Chambre, 2020-2021, 17 mars 2021, no 43, p. 279, Q. no 318)

lnterpellation de N. Boukili au Premier ministre sur 'Smals et les marchés publies relatifs à la digitalisation du service public' (*C.R.I.*, Chambre, 2020-2021, 17 mars 2021, COM 411, p. 31, Q. no 105I)

Question de K. Gabriëls au ministre de la Justice sur 'la numérisation de la Sûreté de l'État' (*C.R.I.*, Chambre, 2020-2021, 17 mars 2021, COM 415, p. 36, Q. no 15422C)

Question de S. Cogolati au ministre de la Justice sur 'les menaces et intimidations du gouvernement turc vis-à-vis d'opposants en Belgique' (*C.R.I.*, Chambre, 2020-2021, 17 mars 2021, COM 415, p. 42, Q. no 15442C)

Questions jointes de B. Pas et K. Metsu au Premier ministre sur 'la menace terroriste croissante en Europe' (*C.R.I.*, Chambre, 2020-2021, 18 mars 2021, PLEN 93, p. 33, Q. nos 1462P et 1471P)

Questions jointes de Ph. Pivin, M. Dillen, N. Boukili, K. Van Vaerenbergh, K. Geens et G. Dallemagne au ministre de la Justice sur 'l'accompagnement et l'indemnisation des victimes d'actes terroristes' (*C.R.I.*, Chambre, 2020-2021, 19 mars 2021, COM 418, p. 1, Q. nos 15257C, 110I, 111I, 15426C, 15448C, 15490C, 15507C, 15511C, 15519C et 15520C)

Suivi des recommandations de la commission d'enquête parlementaire "Attentats terroristes", échange de vues et questions jointes de S. Rohonyi au ministre de la Justice sur 'un fonds d'indemnisation des victimes d'attentats terroristes' (*C.R.I.*, Chambre, 2020-2021, 23 mars 2021, COM 422, p. 1, Q. nos 15751C, 15752C, 15754C, 15755C et 15760C)

Question de Th. Francken au secrétaire d'État à l'Asile et la Migration sur 'le rapatriement d'extrémistes musulmans et de combattants partis en Syrie vers leur pays d'origine' (*C.R.I.*, Chambre, 2020-2021, 26 mars 2021, COM 425, p. 10, Q. n° 15509C)

Questions jointes d'Y. Van Camp, F. Demon, E. Platteau et H. Rigot au secrétaire d'État à l'Asile et la Migration sur 'les équipes outreach actives auprès des migrants en transit' (*C.R.I.*, Chambre, 2020-2021, 26 mars 2021, COM 425, p. 18, Q. n°s 15575C, 15585C, 15851C et 15857C)

Question de B. Segers au secrétaire d'État à l'Asile et la Migration sur 'la plateforme électronique pour les procédures de demande de séjour combinées' (*C.R.I.*, Chambre, 2020-2021, 26 mars 2021, COM 425, p. 43, Q. n° 15814C)

Question de V. Scourneau à la ministre des Affaires étrangères sur 'la sécurité de nos diplomates en République démocratique du Congo' (*Q.R.*, Chambre, 2020-2021, 31 mars 2021, n° 45, p. 99, Q. n° 218)

Question d'A. Ponthier à la ministre des Affaires étrangères sur le 'Congo oriental - assassinat de l'ambassadeur d'Italie' (*Q.R.*, Chambre, 2020-2021, 31 mars 2021, n° 45, p. 113, Q. n° 242)

Question de K. Metsu au ministre de la Justice sur 'le retour des combattants partis en Syrie et le suivi par l'OCAM de femmes et d'enfants liés à Daech' (*C.R.I.*, Chambre, 2020-2021, 31 mars 2021, COM 436, p. 35, Q. n° 15824C)

Question de K. Jadin à la ministre des Affaires étrangères sur 'la terreur de Daech à la prison d'Al-Hol' (*Q.R.*, Chambre, 2020-2021, 7 avril 2021, n° 46, p. 124, Q. n° 228)

Question d'E. Burton à la ministre des Affaires étrangères sur 'les risques pour les diplomates belges en RDC' (*Q.R.*, Chambre, 2020-2021, 7 avril 2021, n° 46, p. 130, Q. n° 248)

Question de M. Freilich au ministre de la Justice sur 'l'entreprise Circles' (*Q.R.*, Chambre, 2020-2021, 7 avril 2021, n° 46, p. 221, Q. n° 378)

Question de M. Vindevoghel au ministre de la Mobilité sur 'la menace terroriste sur le rail' (*Q.R.*, Chambre, 2020-2021, 15 avril 2021, n° 47, p. 122, Q. n° 112)

Question de K. Metsu à la ministre de l'Intérieur sur 'le plan Canal à Bruxelles et la mise en place des CSIL' (*Q.R.*, Chambre, 2020-2021, 15 avril 2021, n° 47, p. 294, Q. n° 400)

Question de B. Segers au secrétaire d'État à l'Asile et la Migration sur 'l'obtention de visas humanitaires par le biais d'intermédiaires' (*Q.R.*, Chambre, 2020-2021, 15 avril 2021, n° 47, p. 352, Q. n° 155)

Question de P. Buysrogge à la ministre de la Défense sur 'les nouveaux minidrones' (*C.R.I.*, Chambre, 2020-2021, 20 avril 2021, COM 438, p. 10, Q. n° 14240C)

Question d'A. Ponthier à la ministre de la Défense sur les suspensions du contrat conclu pour l'Open Source Intelligence System' (*C.R.I.*, Chambre, 2020-2021, 20 avril 2021, COM 438, p. 16, Q. n° 14534C)

Questions jointes de G. Defossé et P. Buysrogge à la ministre de la Défense sur 'les cyberopérations offensives' (*C.R.I.*, Chambre, 2020-2021, 20 avril 2021, COM 438, p. 19, Q. n°s 14627C et 16305C)

Questions jointes de G. Defossé, Ch. Lacroix et K. Verduyckt à la ministre de la Défense sur 'l'extrême droite au sein de l'armée' (*C.R.I.*, Chambre, 2020-2021, 20 avril 2021, COM 438, p. 45, Q. n°s 15600C, 5621C et 16526C)

Question de K. Metsu au ministre de la Justice sur 'l'OCAM' (*C.R.I.*, Chambre, 2020-2021, 21 avril 2021, COM 442, p. 32, Q. n° 16385C)

Question de M. Freilich au ministre de la Justice sur 'le cyberespionnage chinois' (*C.R.I.*, Chambre, 2020-2021, 21 avril 2021, COM 445, p. 33, Q. n° 16518C)

Question de K. Metsu au ministre de la Justice sur 'le cofondateur du CCIB membre du conseil d'administration de Myria et Unia' (*C.R.I.*, Chambre, 2020-2021, 21 avril 2021, COM 445, p. 42, Q. n° 16626C)

Questions jointes d'E. Samyn, K. Aouasti, K. Metsu et Th. Francken à la ministre des Affaires étrangères sur 'les combattantes belges de l'EI en Syrie' (*C.R.I.*, Chambre, 2020-2021, 27 avril 2021, COM 449, p. 33, Q. n^{os} 14807C, 15558C, 15825C et 16400C)

Questions jointes de S. Cogolati, E. Samyn et Ch. Lacroix à la ministre des Affaires étrangères sur 'les menaces et intimidations du gouvernement turc vis-à-vis d'opposants en Belgique' (*C.R.I.*, Chambre, 2020-2021, 27 avril 2021, COM 449, p. 82, Q. n^{os} 15441C, 113I et 16346C)

Débat d'actualité et questions jointes de G. Defossé, J. Pillen, Th. Francken, K. Jadin, Ch. Lacroix et A. Ponthier à la ministre de la Défense sur 'la fin de Resolute Support Afghanistan' (*C.R.I.*, Chambre, 2020-2021, 28 avril 2021, COM 452, p. 1, Q. n^{os} 16438C, 16504C, 16580C, 16622C, 16820C et 16842C)

Question de C. Thibaut à la ministre de l'Intérieur sur 'le contrôle sur les données contenues dans la BNG' (*C.R.I.*, Chambre, 2020-2021, 28 avril 2021, COM 453, p. 16, Q. n^{o} 16719C)

Question d'E. Platteau à la ministre de la Fonction publique sur 'l'arrêt de la Cour constitutionnelle sur le stockage des données de télécommunication' (*C.R.I.*, Chambre, 2020-2021, 28 avril 2021, COM 456, p. 13, Q. n^{o} 16918C)

Question de S. Thémont à la ministre de l'Intérieur sur 'le logiciel de détectage de menaces terroristes ou de radicalisation' (*Q.R.*, Chambre, 2020-2021, 3 mai 2021, n^{o} 50, p. 306, Q. n^{o} 456)

Question de K. Jadin à la ministre de l'Intérieur sur 'le risque d'atteintes aux centres de vaccination' (*Q.R.*, Chambre, 2020-2021, 3 mai 2021, n^{o} 50, p. 313, Q. n^{o} 461)

Interpellation d'E. Gilissen à la ministre de la Fonction publique sur 'l'annulation de la loi sur la conservation des données par la Cour constitutionnelle' (*C.R.I.*, Chambre, 2020-2021, 3 mai 2021, COM 457, p. 1, Q. n^{o} 122I)

Interpellation et questions jointes de K. Bury, S. De Wit, K. Geens et N. Boukili au ministre de la Justice sur 'la législation en matière de conservation des données' (*C.R.I.*, Chambre, 2020-2021, 5 mai 2021, COM 463, p. 1, Q. n^{os} 120I, 16763C, 16799C et 17247C)

Interpellation et questions jointes de K. Jadin et S. Van Hecke au ministre de la Justice sur 'la lutte contre les sectes nuisibles' (*C.R.I.*, Chambre, 2020-2021, 5 mai 2021, COM 463, p. 19, Q. n^{os} 17266C et 17275C)

Question d'E. Platteau à la ministre de l'Intérieur sur 'l'ampleur de la menace que représente l'extrême droite' (*C.R.I.*, Chambre, 2020-2021, 5 mai 2021, COM 464, p. 53, Q. n^{o} 17111C)

Question d'O. Depoortere à la ministre de l'Intérieur sur 'la menace émanant de l'extrême gauche' (*C.R.I.*, Chambre, 2020-2021, 5 mai 2021, COM 464, p. 56, Q. n^{o} 17199C)

Question de K. Metsu à la ministre des Affaires étrangères sur la 'montée en puissance du groupe autoproclamé État islamique au Moyen-Orient' (*Q.R.*, Chambre, 2020-2021, 10 mai 2021, n^{o} 51, p. 140, Q. n^{o} 68)

Question de G. Dallemagne à la ministre de l'Intérieur sur 'la lutte contre le radicalisme durant la période de COVID-19' (*Q.R.*, Chambre, 2020-2021, 10 mai 2021, n^{o} 51, p. 323, Q. n^{o} 470)

Question de V. Scourneau à la ministre des Affaires étrangères sur la 'sécurité informatique' (*Q.R.*, Chambre, 2020-2021, 18 mai 2021, n^{o} 52, p. 117, Q. n^{o} 281)

Question de M. Freilich au ministre de la Justice sur les 'smartphones - Xiaomi, Oppo et OnePlus' (*Q.R.*, Chambre, 2020-2021, 27 mai 2021, n^{o} 53, p. 317, Q. n^{o} 466)

Question de V. Scourneau à la ministre de la Défense sur 'l'achat de drones miniatures par la Défense' (*Q.R.*, Chambre, 2020-2021, 27 mai 2021, n^{o} 53, p. 331, Q. n^{o} 230)

Question de Ch. Lacroix à la ministre de la Défense sur 'le retrait de l'habilitation de sécurité de notre attaché de défense à Paris' (*Q.R.*, Chambre, 2020-2021, 27 mai 2021, n^{o} 53, p. 343, Q. n^{o} 258)

Question de K. Jadin à la ministre de la Défense sur 'les archives de la Défense' (*Q.R.*, Chambre, 2020-2021, 27 mai 2021, n^{o} 53, p. 344, Q. n^{o} 259)

Questions jointes d'E. Gilissen, Y. Ingels, Ph. Pivin, K. Verhelst, F. Demon et M. Freilich à la ministre de l'Intérieur sur 'le piratage du SPF Intérieur' (*C.R.I.*, Chambre, 2020-2021, 27 mai 2021, PLEN 106, p. 13, Q. nos 1679P, 1684P, 1685P, 1686P, 1689P et 1695P)

Questions jointes d'A. Ponthier, S. De Vuyst et P. Buysrogge à la ministre de la Défense sur 'l'affaire Jürgen Conings et la responsabilité de la ministre ainsi que de la Défense' (*C.R.I.*, Chambre, 2020-2021, 27 mai 2021, PLEN 106, p. 101, Q. nos 131I à 133I)

Question de C. Taquin à la ministre de l'Intérieur sur 'l'évaluation du dispositif CSIL-R' (*Q.R.*, Chambre, 2020-2021, 2 juin 2021, no 54, p. 229, Q. no 555)

Débat d'actualité et questions jointes de G. Defossé, P. Buysrogge, Th. Francken, S. De Vuyst, N. Boukili, D. Ducarme, K. Verduyckt, Ch. Lacroix, W. De Vriendt et A. Ponthier à la ministre de la Défense sur 'le suivi du cas du soldat fugitif (*C.R.I.*, Chambre, 2020-2021, 2 juin 2021, COM 495, p. 14, Q. nos 18241C, 18242C, 18309C, 18311C, 18318C, 18320C, 18321C, 18328C, 18388C, 18429C, 18466C et 18482C)

Questions jointes de J. Chanson, E. Platteau, K. Jadin, Ph. Pivin, D. Ducarme et K. Aouasti au Premier ministre sur 'l'extrême droite au sein de la police' (*C.R.I.*, Chambre, 2020-2021, 2 juin 2021, COM 500, p. 7, Q. nos 17992C, 18183C, 18401C, 18420C, 18421C, 18459C et 18460C)

Questions jointes de S. De Vuyst et N. Boukili au Premier ministre sur 'la traque du militaire lourdement armé' (*C.R.I.*, Chambre, 2020-2021, 2 juin 2021, COM 501, p. 14, Q. nos 18075C et 18161C)

Question de N. Boukili au ministre de la Justice sur 'l'espionnage d'un certain nombre de pays européens par les États-Unis' (*C.R.I.*, Chambre, 2020-2021, 2 juin 2021, COM 501, p. 55, Q. no 18457C)

Question de P. De Roover au Premier ministre sur 'les fuites dans la presse au sujet de rapports secrets de la Sûreté de l'État' (*C.R.I.*, Chambre, 2020-2021, 9 juin 2021, COM 511, p. 12, Q. no 15727C)

Question de W. Vermeersch au ministre de la Justice sur 'la reconnaissance des mosquées' (*Q.R.*, Chambre, 2020-2021, 12 juin 2021, no 55, p. 247, Q. no 510)

Question de C. Thibaut au ministre de la Justice sur la 'notification obligatoire pour chaque collaborateur figurant dans une BDC Terrorist Fighters' (*Q.R.*, Chambre, 2020-2021, 12 juin 2021, no 55, p. 274, Q. no 576)

Question de W. Vermeersch à la ministre de l'Intérieur sur 'la reconnaissance des mosquées' (*Q.R.*, Chambre, 2020-2021, 12 juin 2021, no 55, p. 334, Q. no 561)

Question de C. Thibaut à la ministre de l'Intérieur sur 'la manière dont les services de renseignement communiquent avec des instances ou avec des personnes privées ou publiques' (*Q.R.*, Chambre, 2020-2021, 12 juin 2021, no 55, p. 351, Q. no 570)

Questions jointes de N. Boukili, R. Hedebouw et D. Ducarme à la ministre de l'Intérieur sur 'l'affaire Conings' (*C.R.I.*, Chambre, 2020-2021, 16 juin 2021, COM 518, p. 21, Q. nos 18652C, 18653C et 18943C)

Échange de vues et questions jointes de P. Buysrogge, Th. Francken, S. De Vuyst, K. Verduyckt, G. Defossé, M. De Maegd, A. Ponthier, D. Ducarme, Ch. Lacroix et H. Bogaert à la ministre de la Défense sur 'le rapport interne de l'inspection générale de la Défense sur l'affaire Jürgen Conings' (*C.R.I.*, Chambre, 2020-2021, 16 juin 2021, COM 519, p. 1, Q. nos 18607C, 18605C, 18618C, 18656C, 18745C, 18808C, 18835C, 18907C, 18914C, 19011C et 19020C)

Question de Th. Francken au secrétaire d'État à l'Asile et la Migration sur 'l'inspection interne de Fedasil relative aux demandeurs d'asile fauteurs de troubles dans les centres d'accueil' (*C.R.I.*, Chambre, 2020-2021, 18 juin 2021, COM 520, p. 47, Q. no 19059C)

Question de T. Van Grieken au ministre de la Justice sur 'l'agrément des mosquées' (*Q.R.*, Chambre, 2020-2021, 22 juin 2021, no 56, p. 177, Q. no 507)

Question de T. Van Grieken au ministre de la Justice sur le 'screening de demandeurs d'asile concernant des liens avec des groupements terroristes ou des groupements radicaux potentiellement dangereux' (*Q.R.*, Chambre, 2020-2021, 22 juin 2021, nº 56, p. 190, Q. nº 530)

Question de C. Thibaut au ministre de la Justice sur 'la manière dont le SGRS communique avec des instances ou avec des personnes privées ou publiques' (*Q.R.*, Chambre, 2020-2021, 22 juin 2021, nº 56, p. 233, Q. nº 560)

Question de C. Thibaut à la ministre de l'Intérieur sur 'l'évacuation de la ZAD d'Arlon' (*Q.R.*, Chambre, 2020-2021, 22 juin 2021, nº 56, p. 252, Q. nº 578)

Questions jointes de M. De Maegd, M. Ben Achour et P. De Roover à la ministre des Affaires étrangères sur 'la mission belge dans le camp de Roj' (*C.R.I.*, Chambre, 2020-2021, 29 juin 2021, COM 530, p. 89, Q. nºs 18768C, 18798C et 18884C)

Questions jointes d'O. Depoortere, Y. Ingels et T. Vandenput à la ministre de l'Intérieur sur 'le manque d'effectifs à la police' (*C.R.I.*, Chambre, 2020-2021, 30 juin 2021, COM 531, p. 20, Q. nºs 19355C, 19400C et 19429C)

Question d'E. Burton à la ministre des Affaires étrangères sur la 'présence des services des renseignements chinois à Liège' (*Q.R.*, Chambre, 2020-2021, 30 juin 2021, nº 57, p. 118, Q. nº 327)

Question de C. Thibaut au ministre de la Justice sur 'l'évaluation de la menace posée par les anti-5g' (*Q.R.*, Chambre, 2020-2021, 30 juin 2021, nº 57, p. 192, Q. nº 587)

Question de Ph. Pivin au ministre de la Justice sur le 'screening des investissements étrangers – Commission de screening interdépartementale' (*Q.R.*, Chambre, 2020-2021, 30 juin 2021, nº 57, p. 196, Q. nº 597)

Question de D. Safai au secrétaire d'État à l'Asile et la Migration sur 'les visas humanitaires accordés aux femmes et aux enfants liés à l'EI' (*C.R.I.*, Chambre, 2020-2021, 2 juillet 2021, COM 535, p. 21, Q. nº 19570C)

Échange de vues, interpellation et questions jointes de K. Jadin, A. Ponthier, Th. Francken et G. Defossé à la ministre de la Défense sur 'le rapport du Comité R et les soins psychosociaux à l'armée' (*C.R.I.*, Chambre, 2020-2021, 5 juillet 2021, COM 537, p. 1, Q. nºs 18547C, 19099C, 19136C, 00149I, 19252C, 19257C et 19595C)

Question de S. Loones à la ministre du Budget sur 'le budget de la Défense' (*C.R.I.*, Chambre, 2020-2021, 6 juillet 2021, COM 539, p. 20, Q. nº 18077C)

Question d'A. Ponthier au ministre de la Justice sur 'l'influence de Soros' (*Q.R.*, Chambre, 2020-2021, 8 juillet 2021, nº 58, p. 250, Q. nº 595)

Question d'Y. Van Camp au ministre de la Justice sur 'le screening des imams prédicateurs de haine' (*Q.R.*, Chambre, 2020-2021, 8 juillet 2021, nº 58, p. 261, Q. nº 553)

Question de K. Verduyckt au ministre de la Justice sur 'la présence de l'extrême droite dans les rangs du personnel pénitentiaire' (*Q.R.*, Chambre, 2020-2021, 8 juillet 2021, nº 58, p. 268, Q. nº 583)

Question d'A. Van Bossuyt au ministre de la Justice sur 'l'espionnage chinois par le biais du programme Thousand Talents' (*Q.R.*, Chambre, 2020-2021, 8 juillet 2021, nº 58, p. 279, Q. nº 612)

Question de K. Jadin à la ministre de la Défense sur 'le suivi du personnel de la Défense' (*Q.R.*, Chambre, 2020-2021, 8 juillet 2021, nº 58, p. 291, Q. nº 274)

Question de Ph. Pivin à la ministre de l'Intérieur sur la 'Cellule radicalisme de l'Office des étrangers' (*Q.R.*, Chambre, 2020-2021, 8 juillet 2021, nº 58, p. 345, Q. nº 148)

Question de G. Dallemagne au ministre de la Justice sur 'le rapport de l'OCAM sur le wahhabisme, le djihadisme et le terrorisme' (*C.R.I.*, Chambre, 2020-2021, 14 juillet 2021, COM 556, p. 7, Q. nº 19771C)

Questions jointes de J. Pillen, S. Creyelman et K. Jadin à la ministre de la Défense sur 'la composante cyber' (*C.R.I.*, Chambre, 2020-2021, 14 juillet 2021, COM 557, p. 23, Q. nos 17854C, 18003C et 19321C)

Questions jointes de G. Defossé, V. Reynaert et Ch. Lacroix à la ministre de la Défense sur 'la révélation de secrets sur les bombes nucléaires présentes en Europe' (*C.R.I.*, Chambre, 2020-2021, 14 juillet 2021, COM 557, p. 27, Q. nos 18336C, 18384C et 18433C)

Question de Th. Francken à la ministre de la Défense sur 'les opérations psychologiques (psy-ops)' (*C.R.I.*, Chambre, 2020-2021, 14 juillet 2021, COM 557, p. 34, Q. no 18783C)

Interpellations jointes de P. De Roover et B. Pas au Premier ministre sur 'la démission de la commissaire du gouvernement, Mme Haouach' (*C.R.I.*, Chambre, 2021-2022, 15 juillet 2021, PLEN 122, p. 26, Q. nos 162I et 163I)

Question de S. Van Hecke à la ministre des Affaires étrangères sur 'les difficultés de communication avec l'Autorité nationale de Sécurité' (*Q.R.*, Chambre, 2020-2021, 15 juillet 2021, no 59, p. 105, Q. no 341)

Question de C. Thibaut à la ministre des Affaires étrangères sur 'l'absence de réponses de l'ANS au Comité R en matière d'habilitation de sécurité' (*Q.R.*, Chambre, 2020-2021, 15 juillet 2021, no 59, p. 108, Q. no 342)

Question d'Y. Ingels au ministre de la Mobilité sur 'l'octroi des badges d'accès au tarmac' (*Q.R.*, Chambre, 2020-2021, 15 juillet 2021, no 59, p. 185, Q. no 601)

Question de K. Metsu au ministre de la Justice sur 'la reconnaissance des communautés religieuses à Bruxelles' (*Q.R.*, Chambre, 2020-2021, 15 juillet 2021, no 59, p. 261, Q. no 617)

Question de K. Verduyckt à la ministre de l'Intérieur sur 'la présence de l'extrême droite dans les rangs de la police' (*Q.R.*, Chambre, 2020-2021, 15 juillet 2021, no 59, p. 347, Q. no 665)

Échange de vues et questions jointes de B. Pas, E. Samyn, D. Van Langenhove et K. Metsu au Premier ministre et à la ministre des Affaires étrangères sur 'l'opération de rapatriement de femmes et d'enfants de djihadistes' (*C.R.I.*, Chambre, 2020-2021, 22 juillet 2021, COM 560, p. 1, Q. nos 19979C, 19977C, 19981C et 19995C)

Échange de vues et questions jointes de Th. Francken, A. Ponthier, W. De Vriendt, G. Dallemagne, K. Verduyckt, S. De Vuyst, G. Defossé et Ch. Lacroix à la ministre de la Défense sur 'le remplacement du général-major Boucké à la tête du SGRS' (*C.R.I.*, Chambre, 2020-2021, 22 juillet 2021, COM 561, p. 1, Q. nos 19973C, 19974C, 19975C, 19976C, 19983C, 19990C, 19993C et 19994C)

Question d'Y. Ingels à la ministre des Affaires étrangères sur 'l'Autorité Nationale de Sécurité – rôle et missions' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, no 60, p. 92, Q. no 347)

Question de S. Cogolati à la ministre des Affaires étrangères sur 'l'espionnage de la NSA via le Danemark' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, no 60, p. 105, Q. no 363)

Question de K. Jadin à la ministre des Affaires étrangères sur 'l'espionnage de la NSA via le Danemark' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, no 60, p. 109, Q. no 365)

Question de B. Moyaers à la ministre des Affaires étrangères sur 'l'identification politique des pirates informatiques' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, no 60, p. 120, Q. no 376)

Question de S. De Vuyst à la ministre des Affaires étrangères sur 'l'espionnage américain' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, no 60, p. 123, Q. no 380)

Question de C. Taquin au ministre de la Justice sur 'la lutte contre les dérives sectaires durant la pandémie' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, no 60, p. 184, Q. no 567)

Question d'E. Burton au ministre de la Justice sur 'la Sûreté de l'État et l'espionnage' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, no 60, p. 194, Q. no 592)

Question de J. Pillen au ministre de la Défense sur 'l'effectif du SGRS' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, no 60, p. 303, Q. no 286)

Question d'Y. Ingels au Premier ministre sur 'pouvoir échanger en toute sécurité des informations sensibles' (*Q.R.*, Chambre, 2020-2021, 11 août 2021, nº 61, p. 135, Q. nº 111)

Question de D. Safai à la ministre de l'Intérieur sur les 'cours sur le radicalisme et point de contact radicalisation' (*Q.R.*, Chambre, 2020-2021, 11 août 2021, nº 61, p. 337, Q. nº 227)

Échange de vues et questions jointes de Th. Francken, A. Flahaut, G. Liekens, S. de Laveleye, G. Defossé, Ch. Lacroix, V. Reynaert, D. Van Langenhove, W. De Vriendt, Fr. De Smet, H. Rigot, K. Jadin, J. Chanson, T. Vandenput, S. Moutquin, E. Platteau, N. Boukili et B. Segers au Premier ministre sur 'la situation en Afghanistan' (*C.R.I.*, Chambre, 2020-2021, 22 septembre 2021, COM 575, p. 31, Q. nºs 20147C, 20148C, 20156C, 20147C, 20118C, 20094C, 20103C, 20104C, 20140C, 20162C, 20122C, 20154C, 20155C, 20083C, 20093C, 20115C, 20158C, 20137C, 20146C, 20157C, 20057C, 20067C, 20095C, 20110C, 20119C, 20120C, 20127C, 20145C, 20130C, 20132C, 20133C, 20134C, 20135C, 20136C, 20138C, 20139C, 20141C, 20142C, 20161C, 20163C, 20164C et 20165C)

Question de J. Donné au ministre des Finances sur les 'consultations du PCC2' (*Q.R.*, Chambre, 2020-2021, 6 septembre 2021, nº 62, p. 216, Q. nº 146)

Question de W. Vermeersch au ministre des Finances sur la 'reconnaissance des mosquées' (*Q.R.*, Chambre, 2020-2021, 6 septembre 2021, nº 62, p. 228, Q. nº 398)

Question de B. Segers au ministre de la Justice sur le 'screening des candidats à un visa humanitaire' (*Q.R.*, Chambre, 2020-2021, 6 septembre 2021, nº 62, p. 319, Q. nº 606)

Question de M. Freilich au ministre de la Justice sur le 'logiciel de NSO group' (*Q.R.*, Chambre, 2020-2021, 6 septembre 2021, nº 62, p. 337, Q. nº 658)

Question d'Y. Ingels au Premier ministre sur les 'projets de départements de sécurité à la Régie des Bâtiments' (*Q.R.*, Chambre, 2020-2021, 20 septembre 2021, nº 63, p. 338, Q. nº 150)

Questions jointes de Th. Francken, S. Moutquin et D. Van Langenhove au secrétaire d'État à l'Asile et la Migration sur 'le programme de visas humanitaires pour les Afghans' (*C.R.I.*, Chambre, 2020-2021, 22 septembre 2021, COM 575, p. 31, Q. nºs 20703C, 20883C, 20886C, 20888C, 20916C et 20931C)

Questions jointes de M. Freilich, S. Van Hecke, N. Boukili et E. Van Hoof au ministre de la Justice sur 'le logiciel d'écoute' (*C.R.I.*, Chambre, 2020-2021, 22 septembre 2021, COM 577, p. 1, Q. nºs 19985C, 20000C, 20448C et 20845C)

Questions jointes de M. Freilich, E. Gilissen et K. Gabriëls au ministre de la Justice sur 'le classement sans suite dans le cadre de l'enquête sur les espions chinois' (*C.R.I.*, Chambre, 2020-2021, 22 septembre 2021, COM 577, p. 41, Q. nºs 20313C, 20325C et 20903C)

Question de Karin Jiroflée au ministre de la Justice sur 'le non-respect des interdictions temporaires de résidence' (*C.R.I.*, Chambre, 2020-2021, 22 septembre 2021, COM 577, p. 45, Q. nº 20335C)

Débat d'actualité et questions jointes de P. De Roover, K. Jadin, V. Reynaert, H. Rigot et S. Cogolati à la ministre des Affaires étrangères sur 'l'Afghanistan' (*C.R.I.*, Chambre, 2020-2021, 28 septembre 2021, COM 579, p. 7, Q. nºs 20256C, 20270C, 20271C, 20408C, 21142C, 21173C et 21221C)

Questions jointes de S. Van Hecke et E. Van Hoof à la ministre des Affaires étrangères sur 'l'incidence de Pegasus sur les relations diplomatiques et les mesures à prendre dans ce cadre' (*C.R.I.*, Chambre, 2020-2021, 28 septembre 2021, COM 579, p. 19, Q. nºs 20007C et 21061C)

Question de M. Dillen au ministre de la Justice sur 'Oussama Atar et les attentats commis à Paris et Bruxelles' (*C.R.I.*, Chambre, 2020-2021, 29 septembre 2021, COM 586, p. 15, Q. nº 20496C)

Question de Ph. Pivin au ministre de l'Économie sur le 'screening des investissements étrangers – Commission de screening interdépartementale' (*Q.R.*, Chambre, 2020-2021, 2 octobre 2021, nº 64, p. 29, Q. nº 566)

Question de S. Creyelman à la ministre de la Défense sur le 'matériel d'espionnage retrouvé dans l'ambassade de Belgique à Ankara' (*Q.R.*, Chambre, 2021-2022, 2 octobre 2021, nº 64, p. 175, Q. nº 315)

Question de S. Verherstraeten à la ministre de la Défense sur les 'militaires – sympathies pour l'extrême droite' (*Q.R.*, Chambre, 2020-2021, 2 octobre 2021, nº 64, p. 178, Q. nº 320)

Question de D. Safai au secrétaire d'État à l'Asile et la Migration sur 'le rapatriement de terroristes de l'EI et de leurs enfants' (*C.R.I.*, Chambre, 2020-2021, 5 octobre 2021, COM 588, p. 31, Q. nº 20943C)

Question de D. Van Langenhove au secrétaire d'État à l'Asile et la Migration sur 'les résultats du screening de sécurité' (*C.R.I.*, Chambre, 2020-2021, 5 octobre 2021, COM 588, p. 31, Q. nº 20993C)

Question de G. Dallemagne au ministre de la Justice sur 'le noyau salafiste à Molenbeek' (*Q.R.*, Chambre, 2020-2021, 6 octobre 2021, nº 65, p. 422, Q. nº 724)

Question d'E. Van Hoof à la ministre de la Défense sur 'le logiciel espion Pegasus' (*Q.R.*, Chambre, 2020-2021, 6 octobre 2021, nº 65, p. 439, Q. nº 326)

Question de S. Cogolati au ministre de la Justice sur 'l'enquête sur l'attribution de la cyberattaque contre Belnet du 4 mai 2021' (*C.R.I.*, Chambre, 2020-2021, 6 octobre 2021, COM 596, p. 4, Q. nº 21135C)

Question de K. Metsu au ministre de la Justice sur 'les malversations constatées au sein de l'ASBL Exécutif des Musulmans' (*C.R.I.*, Chambre, 2020-2021, 6 octobre 2021, COM 596, p. 26, Q. nº 21579C)

Question de S. Verherstraeten à la ministre de l'Intérieur sur 'la recrudescence de la menace provenant de l'extrême droite' (*C.R.I.*, Chambre, 2020-2021, 6 octobre 2021, COM 597, p. 35, Q. nº 20009C)

Questions jointes de M. Freilich et J. Chanson à la ministre de l'Intérieur sur 'la fin de l'OVG' (*C.R.I.*, Chambre, 2020-2021, 6 octobre 2021, COM 597, p. 55, Q. nºs 20331C et 20404C)

Questions jointes de M. Freilich et K. Metsu à la ministre de l'Intérieur sur 'l'arrestation de plusieurs hommes radicalisés' (*C.R.I.*, Chambre, 2020-2021, 6 octobre 2021, COM 597, p. 76, Q. nºs 20744C, 21288C et 21384C)

Questions jointes d'A. Ponthier, K. Metsu et P. Dewael au Premier ministre sur 'les problèmes récurrents de fondamentalisme au sein de l'Exécutif des Musulmans de Belgique' (*C.R.I.*, Chambre, 2020-2021, 7 octobre 2021, PLEN 127, p. 5, Q. nºs 1932P, 1945P et 1948P)

Question de M. Freilich au Premier ministre sur le 'logiciel de NSO group' (*Q.R.*, Chambre, 2020-2021, 10 octobre 2021, nº 66, p. 39, Q. nº 129)

Débat d'actualité et questions jointes de K. Jadin, A. Ponthier, G. Defossé, Th. Francken et A. FLahaut à la ministre de la Défense sur 'la recherche de l'extrémisme' (*C.R.I.*, Chambre, 2021-2022, 20 octobre 2021, COM 606, p. 1, Q. nºs 20281C, 20292C, 20864C, 20942C,21565C, 22019C et 21674C)

Questions jointes d'A. Ponthier et G. Dallemagne à la ministre de la Défense sur 'les réformes au sein du SGRS après la nomination du vice-amiral W. Robberecht à la tête du service' (*C.R.I.*, Chambre, 2021-2022, 20 octobre 2021, COM 606, p. 10, Q. nºs 20306C et 20923C)

Questions jointes de T. Vandenput et J. Chanson à la ministre de l'Intérieur sur 'les problèmes avec le réseau ASTRID' (*C.R.I.*, Chambre, 2021-2022, 20 octobre 2021, COM 611, p. 40, Q. nºs 21129C et 21212C)

Question de S. Loones à la ministre de l'Intérieur sur 'le signalement de M. Puigdemont dans le système d'information Schengen (SIS)' (*C.R.I.*, Chambre, 2021-2022, 20 octobre 2021, COM 611, p. 53, Q. n° 21308C)

Questions jointes de S. Goethals et O. Depoortere à la ministre de l'Intérieur sur 'la constitution de partie civile de la ministre' (*C.R.I.*, Chambre, 2021-2022, 20 octobre 202, COM 611, p. 66, Q. n°s 21542C et 21575C)

Question d'E. Van Hoof au ministre de la Justice sur 'le logiciel espion Pegasus' (*Q.R.*, Chambre, 2021-2022, 26 octobre 2021, n° 67, p. 247, Q. n° 689)

Question d'A. Ponthier au ministre de la Justice sur le 'coût de l'opération Jürgen Conings' (*Q.R.*, Chambre, 2021-2022, 26 octobre 2021, n° 67, p. 252, Q. n° 699)

Question de S. Creyelman à la ministre de la Défense sur 'la possible divulgation de thèses complotistes par la Russie' (*C.R.I.*, Chambre, 2021-2022, 27 octobre 2021, COM 618, p. 13, Q. n° 22136C)

Questions jointes de G. Defossé et P. Buysrogge à la ministre de la Défense sur 'les propos tenus par M. Lipszyc dans une interview' (*C.R.I.*, Chambre, 2021-2022, 27 octobre 2021, COM 618, p. 21, Q. n°s 22258C et 22364C)

Question de M. Freilich au Premier ministre sur 'la mise à mal du cryptage' (*C.R.I.*, Chambre, 2021-2022, 27 octobre 2021, COM 623, p. 20, Q. n° 22038C)

Question de K. Geens à la ministre de l'Intérieur sur 'l'opération Sky' (*C.R.I.*, Chambre, 2021-2022, 28 octobre 2021, PLEN 136, p. 24, Q. n°s 1990P)

Questions jointes d'A. Ponthier et N. Boukili au ministre de la Justice sur 'les perquisitions menées chez des militaires pour soupçons d'incitation au terrorisme' (*C.R.I.*, Chambre, 2021-2022, 10 novembre 2021, COM 625, p. 15, Q. n°s 22510C et 22521C)

Question de M. Freilich au ministre de la Justice sur 'le logiciel espion développé par NSO' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 257, Q. n° 728)

Question de S. Creyelman à la ministre de la Défense sur les 'extrémisme au sein de la Défense - suivi' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 338, Q. n° 321)

Question de M. Freilich au Premier ministre sur 'l'approche du dark web' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 129, Q. n° 145)

Question de M. Freilich au Premier ministre sur 'la capacité répressive en matière de cybercriminalité' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 130, Q. n° 146)

Question de Th. Francken au ministre de la Justice sur 'le colosse de Molenbeek' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 260, Q. n° 747)

Question de S. Creyelman à la ministre de la Défense sur 'l'extrémisme au sein de la Défense – suivi' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 338, Q. n° 321)

Question de S. Van Hecke à la ministre de la Défense sur 'les actions du SGRS à la suite du projet Pegasus' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 349, Q. n° 355)

Question de S. Matheï au Premier ministre sur 'l'évaluation du RGPD' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 402, Q. n° 221)

Question de K. Jadin à la ministre de la Défense sur 'la sécurité des appareils d'origine chinoise' (*Q.R.*, Chambre, 2021-2022, 25 novembre 2021, n° 70, p. 285, Q. n° 357)

Question d'A. Vicaire au ministre de la Digitalisation sur 'l'affaire Pegasus et la protection des responsables politiques belges' (*C.R.I.*, Chambre, 2021-2022, 30 novembre 2021, COM 630, p. 1, Q. n° 20099C)

Question de K. Metsu au ministre de la Justice sur 'le plan d'action pour la déradicalisation dans nos prisons' (*C.R.I.*, Chambre, 2021-2022, 2 décembre 2021, PLEN 144, p. 15, Q. n° 2090P)

Question d'Y. Ingels au Premier ministre sur la 'politique fédérale en matière de drogues – crime organisé' (*Q.R.*, Chambre, 2021-2022, 6 décembre 2021, n° 71, p. 67, Q. n° 153)

Question de M. Dillen au ministre de la Justice sur le 'rapport de la Cour des comptes sur l'ASA – objectifs transversaux de simplification administrative' (*Q.R.*, Chambre, 2021-2022, 6 décembre 2021, nº 71, p. 225, Q. nº 796)

Question d'E. Burton au ministre de la Justice sur 'les deepfakes' (*Q.R.*, Chambre, 2021-2022, 6 décembre 2021, nº 71, p. 248, Q. nº 823)

Question de S. Cogolati au ministre de la Justice sur 'les risques d'espionnage au China-Belgium Technology Center' (*Q.R.*, Chambre, 2021-2022, 6 décembre 2021, nº 71, p. 250, Q. nº 824)

Questions jointes B. Pas et K. Metsu au Premier ministre sur 'le suivi défaillant des djihadistes en Belgique' (*C.R.I.*, Chambre, 2021-2022, 9 décembre 2021, PLEN 145, p. 23, Q. nºs 2099P et 2124P)

Questions jointes de K. Jadin et M. Vindevoghel à la ministre de la Défense sur 'le recrutement du militaire belge' (*C.R.I.*, Chambre, 2021-2022, 15 décembre 2021, COM 640, p. 3, Q. nºs 23244C et 23388C)

Question de G. Defossé à la ministre de la Défense sur 'les menaces de mort proférées par un militaire belge contre un ministre' (*C.R.I.*, Chambre, 2021-2022, 15 décembre 2021, COM 640, p. 7, Q. nº 23346C)

Question de K. Jadin à la ministre de l'Intérieur sur 'l'extrémisme en Belgique' (*C.R.I.*, Chambre, 2021-2022, 15 décembre 2021, COM 642, p. 6, Q. nº 23074C)

Question d'E. Platteau à la ministre de l'Intérieur sur 'la lutte contre l'extrémisme au travers de la réinsertion sociale et du désengagement' (*C.R.I.*, Chambre, 2021-2022, 15 décembre 2021, COM 642, p. 13, Q. nº 23104C)

Questions jointes d'E. Platteau, F. Demon, T. Vandenput et O. Depoortere à la ministre de l'Intérieur sur 'le rapport de l'OCAM sur la crise du coronavirus ' (*C.R.I.*, Chambre, 2021-2022, 15 décembre 2021, COM 642, p. 14, Q. nºs 23178C, 23229C, 23393C et 23415C)

Questions jointes K. Metsu et Ph. Pivin au ministre de la Justice sur 'l'Exécutif des Musulmans de Belgique' (*C.R.I.*, Chambre, 2021-2022, 16 décembre 2021, PLEN 148, p. 15, Q. nºs 2131P et 2143P)

Questions jointes K. Metsu et B. Pas au ministre de la Justice sur 'la communication d'informations erronées au Parlement' (*C.R.I.*, Chambre, 2021-2022, 16 décembre 2021, PLEN 148, p. 15, Q. nºs 206I et 214I)

Question de S. Cogolati à la ministre de la Fonction publique sur 'les risques de censure et cybersurveillance sur les smartphones Huawei, Xiaomi et One Plus' (*Q.R.*, Chambre, 2021-2022, 16 décembre 2021, nº 72, p. 180, Q. nº 349)

Question de S. Creyelman à la ministre de la Défense sur 'le développement de la composante Cyber au sein de la Défense' (*Q.R.*, Chambre, 2021-2022, 16 décembre 2021, nº 72, p. 228, Q. nº 346)

Question de Th. Francken à la ministre de l'Intérieur sur 'la vérification lors de l'opération d'évacuation' (*Q.R.*, Chambre, 2021-2022, 16 décembre 2021, nº 72, p. 335, Q. nº 386)

Question de G. Dallemagne à la ministre de l'Intérieur sur 'le rapport annuel de la Sûreté de l'État' (*C.R.I.*, Chambre, 2021-2022, 20 décembre 2021, COM 645, p. 2, Q. nº 22634C)

Question de K. Bury au ministre de la Justice sur 'l'achat d'immeubles de bureaux dans le quartier Nord à Bruxelles' (*C.R.I.*, Chambre, 2021-2022, 20 décembre 2021, COM 645, p. 26, Q. nº 23267C)