COMITÉ PERMANENT DE CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ

RAPPORT D'ACTIVITÉS 2023

Conception graphique et mise en page : Imprimerie centrale de la Chambre des Représentants

Conformément à l'article 35 de la Loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace,

§ 1er. Le Comité permanent R fait rapport à la Chambre des Représentants et au Sénat dans les cas suivants : 1° annuellement, par un rapport général d'activités qui comprend, s'il échet, des conclusions et des propositions d'ordre général et qui couvre la période allant du 1er janvier au 31 décembre de l›année précédente. Ce rapport est transmis aux Présidents de la Chambre des représentants et du Sénat ainsi qu'aux ministres compétents le 1er juin au plus tard. Dans ce rapport, le Comité permanent R consacre une attention spécifique aux méthodes spécifiques et exceptionnelles de recueil de données, telles qu'elles sont visées dans l'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, à l'application du chapitre IV/2 de la même loi et à la mise en œuvre de la loi du 10 juillet 2006 relative à l'analyse de la menace. [...]

§ 2. Le Comité permanent R fait rapport à la Chambre des représentants annuellement 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. Copie de ce rapport annuel est également adressée aux Ministres de la Justice et de la Défense ainsi qu'à la Sûreté de l'Etat 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. 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. Il précise également les activités du Comité permanent R. Les éléments figurant dans le rapport ne peuvent pas porter atteinte au bon fonctionnement des services de renseignement et de sécurité ou mettre en danger la collaboration entre les services de renseignement et de sécurité belges et étrangers.

§ 3. 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. Copie de ce rapport est également adressée aux ministres compétents, ainsi qu'à la Sûreté de l'Etat 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.

Bruxelles, 23 avril 2024

Serge Lipszyc
Président

Linda Schweiger
Conseillère

Séverine Merckx
Conseillère

Frédéric Givron
Greffier

PREFACE

Rédiger pour la dernière fois la préface du Rapport annuel 2024 du Comité permanent R, c'est revenir sur les années durant lesquelles j'ai occupé la présidence du Comité R. C'est l'occasion de partager une série de constats.

Le terrorisme sous toutes ses formes reste présent. Il nécessite de l'État un investissement sans faille dans toutes ses structures.

Nous assistons au renforcement de la Sureté de l'Etat, du Service Général de Renseignement et Sécurité (SGRS) et encore de l'OCAM. Nous observons, plus généralement, le besoin de renforcer leur appui aux structures locales de coordination, comme leur collaboration en matière judiciaire.

Ces décisions sont louables. Elles doivent se poursuivre dans la durée. En ces temps incertains, le renforcement de notre sécurité constitue plus qu'une obligation pour l'État.

Nous avons été témoins de la résurgence de la violence de l'extrême droite notamment à l'occasion de l'affaire Jürgen Conings, ainsi que d'une série d'autres actes commis à l'encontre de la Défense notamment. La crise de la Covid a été le catalyseur pour d'autres atteintes aux structures étatiques.

Les risques liés au renforcement des Frères musulmans en Belgique ne semblent pas toujours pris à leur juste mesure.

L'attentat du 16 octobre 2023 contre des supporters suédois nous rappelle à quel point nous restons exposés.

L'ingérence étrangère a trouvé au sein des différents parlements européen, fédéral ou régional une caisse de résonance sans pareil et constitue assurément un enjeu démocratique considérable avec la mise en cause de certains parlementaires. Mais les actions en cours découvrent-elles le sommet de l'iceberg ou une simple péripétie ?

Cette dangerosité a été bousculée par les risques accrus d'organisation criminelle se développant en raison de leurs activités dans le trafic international de stupéfiants et la corruption qui en résultait.

Ce phénomène des plus inquiétants amène la Sûreté de l'État à investir ce domaine. Mais il a également poussé le gouvernement à étendre le screening aux personnels des ports comme cela avait déjà été décidé pour d'autres domaines, comme la Défense, ceux du ferroviaire, des communications, des agents pénitentiaires…

La résurgence des conflits armés nous a rappelé la nécessité de réagir face aux risques de départ d'hommes et de femmes vers ces zones de guerre.

Nous ne pouvons oublier la fragilité de nos institutions face à l'espionnage.

Notre pays, comme beaucoup d'autres démocraties, sont à la merci de tentatives de désinformation étatique initiées par des puissances étrangères. Ce danger est encore plus grand à la veille des élections du 9 juin 2024.

La Belgique est assurément attractive et ce d'autant plus que nombres d'institutions internationales ont leur siège chez nous.

Les services de renseignement doivent donc redoubler leurs efforts tant les menaces sont multiples.

La Défense a donné naissance au Cyber Command, responsable de la cybersécurité des réseaux et systèmes d'armes employés par la Défense. Il collecte l'information au profit du SGRS. Outil indispensable pour notre sécurité, il permettra certainement de récupérer notre retard en la matière. Il importe que, demain, il reste bien sous l'autorité du SGRS et sous le contrôle du Comité comme aujourd'hui.

Le renforcement de la sécurité ne peut faire l'impasse de celui des droits des citoyens. Des enjeux considérables s'ouvrent à nous en raison de l'intelligence artificielle mais aussi des nouvelles technologies d'intrusion dans notre vie privée qui sont aujourd'hui indétectables.

Les services de renseignement doivent améliorer leurs partenariats en Belgique comme à l'étranger.

Les failles et échecs résultent avant tout de l'existence de «silos» entre services et d'une certaine résistance au partage de l'information.

Dans ce contexte, le Comité R est à la croisée des chemins, il a vu la désignation de deux nouvelles conseillères, l'arrivée d'une nouvelle génération de collaborateurs mais aussi l'augmentation notable de ses compétences, comme l'importance accrue de l'Organe de recours dans le domaine de la sécurité.

Aujourd'hui, je termine mon mandat en adressant mes vifs remerciements à ces collaborateurs, à ces Femmes et ces Hommes qui m'ont fait confiance et m'ont soutenu dans ma quête du bien commun et d'une plus grande liberté.

J'ai eu la chance de partager ces valeurs avec beaucoup d'autres, mes pensées vont également à eux, car nous avons œuvré, chacun avec nos possibilités, pour un monde plus juste.

Bruxelles, 18 avril 2024.

Serge Lipszyc
Président du Comité Permanent de Contrôle des services de renseignement et de sécurité

TABLE DE MATIÈRES

1. ENQUÊTES DE CONTRÔLE

ENQUÊTES DE CONTRÔLE

Enquêtes de contrôle clôturées[1]

Les fonds spéciaux

À l'instar de tout service public, les services de renseignement se voient également allouer des fonds publics pour exercer leurs missions légales. Ces fonds doivent faire l'objet d'une transparence parfaite et d'un contrôle total. Cependant, comme certaines tâches de la VSSE et du SGRS doivent être tenues secrètes, une partie de leur budget échappe à cette règle. Ces dépenses sont mieux connues 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. Précédemment, le Comité s'est 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 internes (au sein des services) qu'externes (Cour des comptes, Inspection des Finances, Comité permanent R). Depuis 2018 (pour la VSSE) et 2020 (pour le SGRS), la Cour des comptes réalise un contrôle périodique de ces fonds. Dans ce contexte, la Cour des comptes fait appel à l'assistance technique du Comité permanent R. Le Comité peut à son tour exercer sa mission avec plus d'attention sur l'utilisation de ces dits fonds. Le Comité peut 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. Au terme de son enquête, le Comité a constaté les progrès réalisés par les deux services dans le contrôle de ces fonds tout en identifiant encore certaines pistes d'amélioration, telles que la définition de critères précis pour l'utilisation de ces fonds.

Le financement des partis politiques

Avec la Loi du 4 juillet 1989 relative à la limitation et au contrôle des dépenses électorales (*M.B.* 20 juillet 1989), la Belgique a mis en place un dispositif de financement public direct des partis politiques. En contrepartie de ce financement, elle leur impose des obligations précises : le plafonnement des dépenses de propagande électorale ; la réglementation de l'utilisation de certains moyens électoraux ; l'interdiction des dons de personnes morales et d'associations de fait, ainsi que la limitation et l'identification des dons de personnes physiques ; la transparence de la comptabilité et le respect des droits et libertés garantis par la Convention européenne des droits de l'Homme. A la suite des révélations parues fin 2022 dans la presse belge et européenne autour d'une ingérence financière russe, Le Comité a réalisé une analyse juridique des règles existantes permettant la détection, par les services de renseignement, de financements étrangers irréguliers visant à influencer les politiciens belges.

La Convention 108+

Dans le domaine du renseignement, les droits des personnes concernées par des traitements de données et la transparence à leur égard sont significativement limités en raison de l'impératif de confidentialité des activités des services de renseignement. En effet, les instruments européens, comme le Règlement général de protection des données ou la Directive « Police Justice », ne s'appliquent pas aux traitements de données réalisés dans le domaine de la sécurité nationale. Dans cette matière, le seul instrument international juridiquement contraignant est la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (la « Convention 108 ») de 1981. En 2018, la Convention 108 a été amendée en « Convention 108+ » qui précise et renforce le cadre juridique en matière de données à caractère personnel dans le domaine de la sécurité nationale.

Dans une enquête de contrôle, le Comité mettait en avant les opportunités liées à la ratification de la Convention 108+ et à l'adaptation du cadre juridique national, sans minimiser les contraintes pour les services de renseignement et de sécurité.

Par exemple, la Convention 108+ invite à réexaminer la manière dont s'exerce le droit d'accès indirect aux données à caractère personnel ainsi que les procédures d'accès aux informations détenues par les services et les exceptions à la communication de ces informations. De telles mesures renforceraient la confiance du citoyen et permettraient un contrôle plus efficace. La Convention 108+ donne en effet l'occasion au législateur de confier aux organes de contrôle les moyens de vérifier l'effectivité du régime des flux transfrontières à l'égard des services, de revoir les exceptions permettant de procéder à un transfert de données en l'absence de niveau approprié de protection et de fixer dans la loi les principes applicables à la coopéra-

1 Les versions intégrales des rapports d'enquête sont consultables sur www.comiteri.be.

tion internationale des services. Enfin, la Convention 108+ met en place un mécanisme de coopération et d'entraide entre les autorités de contrôle. Plus spécifiquement, le texte prévoit la possibilité de coordonner les interventions des autorités de contrôle, d'agir conjointement, et d'échanger des informations.

Si les règles de protection des données peuvent être ressenties par les services comme autant de freins dans l'exercice de leurs missions, ces précisions au cadre normatif et ce renforcement de la transparence contribuent à la légitimité de leur action.

Si la Belgique a signé la Convention 108+ en octobre 2018, elle ne l'a pas encore ratifiée. À la suite de son analyse juridique, le Comité permanent R soulignait la grande plus-value de la Convention 108+ et invitait les Ministres de la Justice et de la Défense, compétents pour les services de renseignement et de sécurité, à interpeller la Ministre des Affaires étrangères en vue de sa ratification.

TikTok et les risques de sécurité

En mars 2023, le Conseil national de Sécurité prenait la décision d'interdire temporairement l'utilisation de TikTok sur les appareils des services publics, invoquant des préoccupations relatives à la vie privée et à la sécurité. À la demande de la Commission de suivi, le Comité permanent R a réalisé une note analysant la position d'information des services de renseignement sur cette problématique. Les deux services alertaient ainsi sur les vulnérabilités techniques de l'application ainsi que sur la collecte et le partage de (méta)données, notamment avec les autorités chinoises. L'analyse du Comité offrait également un aperçu des mesures nationales prises par les Etats membres de l'Union européenne visant à restreindre l'accessibilité de l'application.

Le suivi d'un imam

Figure emblématique de la scène religieuse bruxelloise, un imam marocain a fait l'objet en octobre 2021 d'une décision de retrait de permis de séjour. Cette décision a été justifiée par le Secrétaire d'Etat à l'Asile et à la Migration à partir de renseignements fournis par la VSSE. Quelques jours plus tôt, ces mêmes informations avaient toutefois été jugées insuffisamment étayées par le Tribunal de la Famille de Bruxelles qui avait fait droit à la demande d'acquisition de la nationalité belge de l'imam.

En février 2022, le Comité a ouvert une enquête visant à examiner la position d'information de la VSSE, les moyens mis en œuvre dans le suivi de l'intéressé ainsi que le traitement et le partage de données à caractère personnel par la VSSE à d'autres autorités et administrations. L'enquête a permis de clarifier les actions entreprises par la VSSE dans le cadre de deux procédures parallèles concernant l'imam : d'une part, la VSSE a rendu un avis relatif à la déclaration de nationalité introduite par l'intéressé et, d'autre part, le service de renseignement a répondu à une demande d'informations de la part de l'Office des Etrangers suite à la médiatisation, en janvier 2019, d'un ancien prêche de l'imam. Ces deux procédures concomitantes ont été perçues par la VSSE comme une opportunité pour la mise en œuvre de sa « stratégie d'entrave » (voir *infra*). Plus particulièrement dans ce dossier, la VSSE a partagé des renseignements à l'Office des Etrangers avec pour objectif le retrait du permis de séjour de l'intéressé.

Au terme de son enquête, le Comité a constaté des dysfonctionnements dans la gestion du dossier de l'intéressé au sein de la VSSE. En effet, dans sa communication externe, le service a partagé des conclusions sévères que le Comité a jugé non proportionnées au regard des informations récoltées et de la stratégie de suivi mise en œuvre Le Comité a formulé plusieurs recommandations, tout en saluant les efforts déjà entrepris par la VSSE pour améliorer son fonctionnement interne. En sa qualité d'autorité de contrôle compétente (art. 95 LPD), le Comité permanent R a ordonné des mesures correctrices.

Les screenings de sécurité

Par le passé, le Comité permanent R, dont le Président est également Président de l'Organe de recours en matière d'habilitations, attestations et avis de sécurité, a formulé de nombreuses recommandations relatives aux screenings de sécurité, par exemple à propos des nécessaires screenings de sécurité pour certaines fonctions de confiance, ou pour les militaires et civils de la Défense, ou encore quant à l'application conforme de la possibilité d'introduire des demandes de screenings de sécurité.

Plusieurs recommandations ont également été formulées dans le cadre d'une enquête plus globale sur les screenings de sécurité (2019), plusieurs recommandations ont également été formulées. Le Comité y a soulevé la question du pré-screening des candidats à des emplois au sein de la VSSE et a décidé, en sa qualité d'autorité de contrôle compétente, d'y dédier une enquête. Après analyse des procédures existantes au sein de la VSSE et du SGRS, le Comité recommandait d'uniformiser la procédure des vérifications de sécurité pour tous les candidats à un emploi au sein d'un des services de renseignement ou de l'OCAM.

Une plainte de l'Exécutif des Musulmans

Début 2022, l'Exécutif des Musulmans de Belgique (EMB) a déposé une plainte « *concernant le fonctionnement de la Sûreté de l'Etat, plus particulièrement la fuite systématique de rapports et la consultation de rapports par des journalistes alors que les intéressés visés par ces rapports n'ont pas cette possibilité* » (traduction libre). L'EMB affirmait que des rapports et notes de la Sûreté de l'Etat sont souvent utilisés pour discréditer les Musulmans et les mosquées. Ces notes fuitées créeraient une image négative et stigmatisante (permanente) de l'Islam et des Musulmans.

La fuite systématique vers les médias constitue, selon l'EMB, une atteinte à la vie privée des personnes qui font l'objet de ces rapports (art. 22 de la Constitution et art. 8 CEDH). Au terme de son enquête, le Comité émettait certaines réserves sur la gestion passée des fuites d'informations au sein de la VSSE mais se réjouissait de la publication de nouvelles directives internes, prévoyant notamment la rédaction d'un rapport écrit sur tout incident de sécurité détecté. Le Comité rappelait toutefois l'obligation légale de la VSSE de signaler les brèches de sécurité de données personnelles au Comité, en sa qualité d'autorité de contrôle compétente.

Entrave

L'an dernier, le Comité a réalisé une analyse juridique des options légales dont disposent les services de renseignement en matière d'entrave (ou *disruption*), c'est-à-dire la perturbation d'une menace en vue de la faire disparaitre ou d'en réduire l'impact. Cette analyse visait à clarifier une question soulevée dans plusieurs dossiers examinés par le Comité.

A travers cette analyse, le Comité souhaitait notamment examiner la manière dont la VSSE organise sa stratégie d'« entrave ». Le Comité s'est concentré sur l'étude du cadre réglementaire interne et son adéquation au cadre légal, sans examiner, à ce stade, l'opérationnalisation, par la VSSE, de sa stratégie de *disruption*. L'analyse a également porté sur les conditions auxquelles le SGRS est autorisé à entraver les menaces.

Le risque d'infiltration au sein des services

Le monde du renseignement, au niveau international, a été secoué ces dernières années par une série de cas d'infiltration au sein même des services *('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 en leur sein : quels risques ont été identifiés ? Quelles mesures ont été prises pour les maîtriser et pour réagir si ces risques venaient à se concrétiser ? Étant donné l'importance et la sensibilité de ce dossier, le Comité a décidé fin 2023 d'opter pour une analyse « continue » de cette problématique et du suivi qu'en font les services.

L'évaluation par l'OCAM de la menace sur une délégation iranienne à Bruxelles

En juin 2023 avait lieu le *Brussels Urban Summit*, réunion internationale des maires des grandes villes. À cette occasion, des représentants de plus de 300 villes étaient invités à Bruxelles. Dans ce cadre, des visas « à territorialité limitée » ont été octroyés par la Belgique aux quatorze membres d'une délégation iranienne, dont le maire de Téhéran. L'octroi de ces visas, quelques semaines après la libération d'un citoyen belge, a fait l'objet d'un vif débat parlementaire. Les révélations quant aux activités présumées de surveillance et d'espionnage d'opposants iraniens par des membres de cette délégation ont encore alimenté la controverse politico-médiatique.

Dans ce contexte, à la demande de la Commission d'accompagnement, les Comités permanents P et R ont ouvert une enquête de contrôle commune relative à la position d'information et à l'implication de l'OCAM dans ce dossier. Les Comités ont ainsi constaté que l'OCAM n'est intervenu qu'après la délivrance des visas aux membres de la délégation iranienne en vue de répondre aux demandes d'évaluation de la menace du Centre de crise national.

Plus précisément, la double évaluation de l'OCAM concernait une éventuelle menace portant sur l'événement du *Brussels Urban Summit* ainsi que plus particulièrement sur le maire de Téhéran. L'OCAM n'a donc pas été interrogé sur la menace que pouvait représenter ou non (certains membres de) la délégation iranienne. L'OCAM n'a pas non plus pris l'initiative de réaliser une telle évaluation.

Étant donné le champ de compétences de l'Organe de Coordination, cette analyse se serait limitée aux potentielles menaces extrémistes et terroristes. L'enquête des Comités permanents P et R a toutefois permis de clarifier le fait que l'OCAM ne disposait d'aucune information quant à une menace dirigée contre ou émanant de la délégation iranienne.

Enquêtes de contrôle en cours

Accès aux images des caméras de police

Conformément à la Loi organique des services de renseignement et à la Loi sur la fonction de police, les services de renseignement peuvent avoir accès, sous réserve de certaines conditions, aux images des caméras de vidéosurveillance des services de police. Alerté par le chef de corps d'une zone de police locale, le Comité cherche à clarifier les modalités pratiques d'accès aux images des caméras de police par les services de renseignement. En effet, le chef de corps faisait état d'accords avec des zones de police en vue de l'accès aux données à distance. Le cadre légal prévoit la consultation des images *in situ*, en présence d'un opérateur policier dans le centre de gestion des images au sein de la zone de police. Le Comité a jugé qu'une analyse juridique s'imposait afin d'assurer la sécurité juridique de tous les acteurs impliqués.

Des méthodes (particulières) de renseignement

Le Comité dispose d'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 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 à la prise d'images animées (art. 44/3 L.R&S). Le Comité a décidé d'étudier cette matière en profondeur, en ce qui concerne tant l'exécution de ces méthodes par les services de renseignement que les modalités pratiques de son contrôle.

Méthodologie d'analyse

Dans le cadre de ses enquêtes de contrôle ou à travers le traitement de plaintes, le Comité est souvent confronté à des dossiers dans lesquels les services de renseignement attribuent des qualifications à des individus et les relient à une menace. De telles qualifications sont parfois contestées par les intéressés. Le Comité a ouvert une enquête en vue de comprendre la méthodologie mise en œuvre par les services de renseignement pour qualifier une « *person of interest* ». En parallèle, la méthodologie d'analyse utilisée par l'OCAM est examinée conjointement avec le Comité permanent P.

Une brèche de sécurité

Certaines fuites de données impliquent l'obligation de notifier le Comité permanent R, en sa qualité d'Autorité de contrôle compétente dans le cadre du traitement des données à caractère personnel par les services de renseignement, dès qu'il existe un risque pour les droits et libertés des personnes dont les données à caractère personnel ont fuité. En 2023, le Comité a ouvert une enquête de contrôle à la suite d'une potentielle soustraction frauduleuse de données.

Le suivi d'une délégation iranienne à Bruxelles par la VSSE et le SGRS

En juin 2023 avait lieu à Bruxelles une réunion internationale des maires des grandes villes. Dans ce cadre, des visas à validité territoriale ont été octroyés par la Belgique aux quatorze membres d'une délégation iranienne. À la demande de la Commission d'accompagnement, l'enquête examine notamment le rôle joué par les services de renseignement dans le processus de screening en vue de la délivrance de ces visas. Une enquête similaire a été menée avec le Comité permanent P concernant le rôle de l'OCAM dans ce dossier (*supra*).

Les menaces liées au régime iranien

Au-delà du dossier spécifique de la délégation iranienne présente à Bruxelles en juin 2023, la Commission d'accompagnement a invité le Comité à enquêter sur la manière dont les services de renseignement suivaient « *les activités du régime iranien* ». Cette enquête analyse dès lors le cadre légal et les moyens dédiés à cette matière au sein des services de renseignement. Une enquête distincte, menée conjointement avec le Comité permanent P, examine l'évaluation de la menace, par l'OCAM, à l'égard des « opposants à des régimes autoritaires présents en Belgique ».

L'attaque terroriste sur des supporters suédois

En octobre 2023, en marge du match de football Belgique-Suède, un attentat terroriste dans le centre de Bruxelles a fait deux morts et un blessé, tous trois Suédois. L'auteur de l'attentat a été rapidement identifié. Le Comité a ouvert deux enquêtes de contrôle dans lesquelles sont examinées, d'une part, la position d'information des services de renseignement sur l'intéressé et d'autre part, dans le cadre d'une enquête menée conjointement avec le Comité permanent P, celle de l'OCAM.

L'ingérence de puissances étrangères

A la demande de la Commission d'accompagnement, le Comité a ouvert une enquête de contrôle relative aux actions entreprises par les services de renseignement et de sécurité afin de détecter la menace d'ingérence, par des puissances étrangères, via le financement de partis, d'institutions et/ou de figures politiques en Belgique.

2. TRAITEMENT DES PLAINTES

TRAITEMENT DES PLAINTES

Outre les enquêtes de contrôle, le Comité traite également des plaintes et dénonciations relatives au fonctionnement, à l'intervention, à l'action ou à l'absence d'action des services de renseignement, de l'OCAM et de ses services d'appui et de leurs membres. Le Comité est en outre 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. Il agit alors en qualité d'autorité de protection des données à laquelle le requérant peut demander la vérification du respect des règles d'application en matière de protection des données ainsi que la rectification ou la suppression de ses données.

2023	COMITE PERMANENT R		COMITES PERMANENTS P & R	TOTAL
1. Plaintes introduites 2023	55		2	57
2. Plaintes irrecevables 2023	40		0	40[1]
3. Plaintes recevables 2023	21		2	23
	VSSE	14		
	SGRS	3		
	VSSE/SGRS	4		
4. Plaintes DPA recevables 2023	17		2	19
5. Plaintes en suspens	6		0	6[2]
6. Plaintes en cours	10		2	12[3]
7. Plaintes recevables clôturées	37		6	43[4]
8. Mesures correctrices	3		0	3[5]
9. Total des plaintes recevables traitées	53		8	61[6]

1 Dont 9 plaintes introduites en 2022.
2 Dont 3 plaintes en attente d'une décision de recevabilité.
3 Dont 1 plainte de 2020 et 11 plaintes de 2023.
4 Dont 8 plaintes de 2021, 26 plaintes de 2022 et 9 plaintes de 2023. À cela s'ajoutent les 40 plaintes jugées irrecevables.
5 Dont 2 plaintes de 2022 et 1 plainte de 2023.
6 Somme des plaintes en suspens, en cours et clôturées. À cela s'ajoutent les 40 plaintes jugées irrecevables.

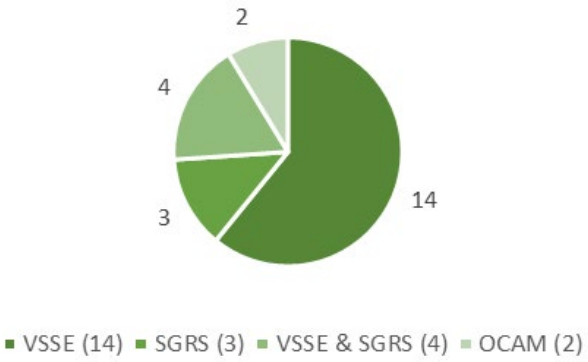
Le tableau ci-dessus donne un aperçu des dossiers traités (ouverts et/ou clôturés) en 2023. Les colonnes du tableau ventilent les plaintes selon que la compétence du Comité permanent R est exclusive ou conjointe avec le Comité permanent P. Il convient de noter qu'une seule et même plainte peut constituer plusieurs « dossiers » selon les services visés : une plainte visant l'OCAM et la VSSE sera par exemple comptabilisée à la fois dans les dossiers traités conjointement par les Comités permanents P et R pour le volet OCAM de l'enquête et dans les dossiers traités exclusivement par le Comité permanent R pour les devoirs d'enquêtes portant sur la VSSE.

En 2023, le Comité permanent R a reçu, au total, 55 plaintes ou dénonciations. Après une brève pré-enquête et la vérification de plusieurs données objectives, le Comité a rejeté 40 plaintes ou dénonciations parce qu'elles étaient manifestement non fondées, ou parce que le Comité n'était pas compétent pour en traiter les griefs. Dans ce dernier cas de figure, les plaignants ont été renvoyés vers les instances compétentes lorsque celles-ci pouvaient être identifiées (par exemple, le ministère public, l'Organe de contrôle de l'information policière ou le Comité permanent P).

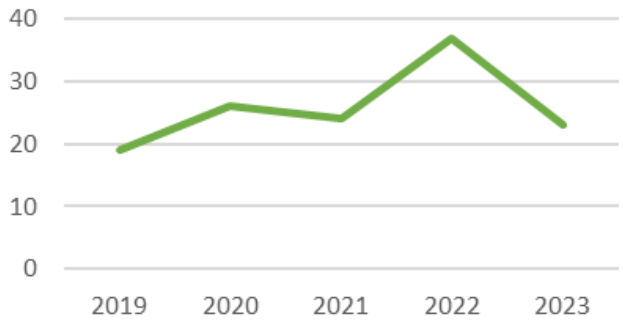
Parmi les plaintes recevables introduites en 2023, 19 dossiers ont été traités en tant que plaintes DPA *(Data Protection Authority)*. Cette année encore, le Comité a ainsi eu à traiter plusieurs requêtes déposées dans le cadre de procédures administratives (déclaration de nationalité, droit de séjour, etc.). Confrontés à une décision négative motivée sur la base d'informations fournies par VSSE, le SGRS et/ou l'OCAM, les requérants s'adressent (entre autres) au Comité permanent R pour un contrôle du traitement de leurs données à caractère personnel. Les modalités de partage de ces données avec des partenaires étrangers attirent également de plus en plus l'attention du Comité, saisi par des requérants ayant rencontré des problèmes à l'étranger lors d'un contrôle aux frontières. En sa qualité d'autorité de contrôle, le Comité permanent R a ordonné des mesures correctives à l'égard des services de renseignement concernés dans trois dossiers (art. 51/3 L.Contrôle). Selon les dossiers, il peut s'agir d'exiger la rectification voire la suppression de données à caractère personnel, la notification de la décision du Comité aux partenaires et/ou aux autorités ou encore la diffusion de la décision au sein du service concerné. Dans le contexte de signalements internationaux, le Comité constate que des limites subsistent aux demandes de correction puisque celles-ci dépendent également du bon vouloir des services partenaires étrangers, étant entendu que la coopération est parfois limitée, voire inexistante.

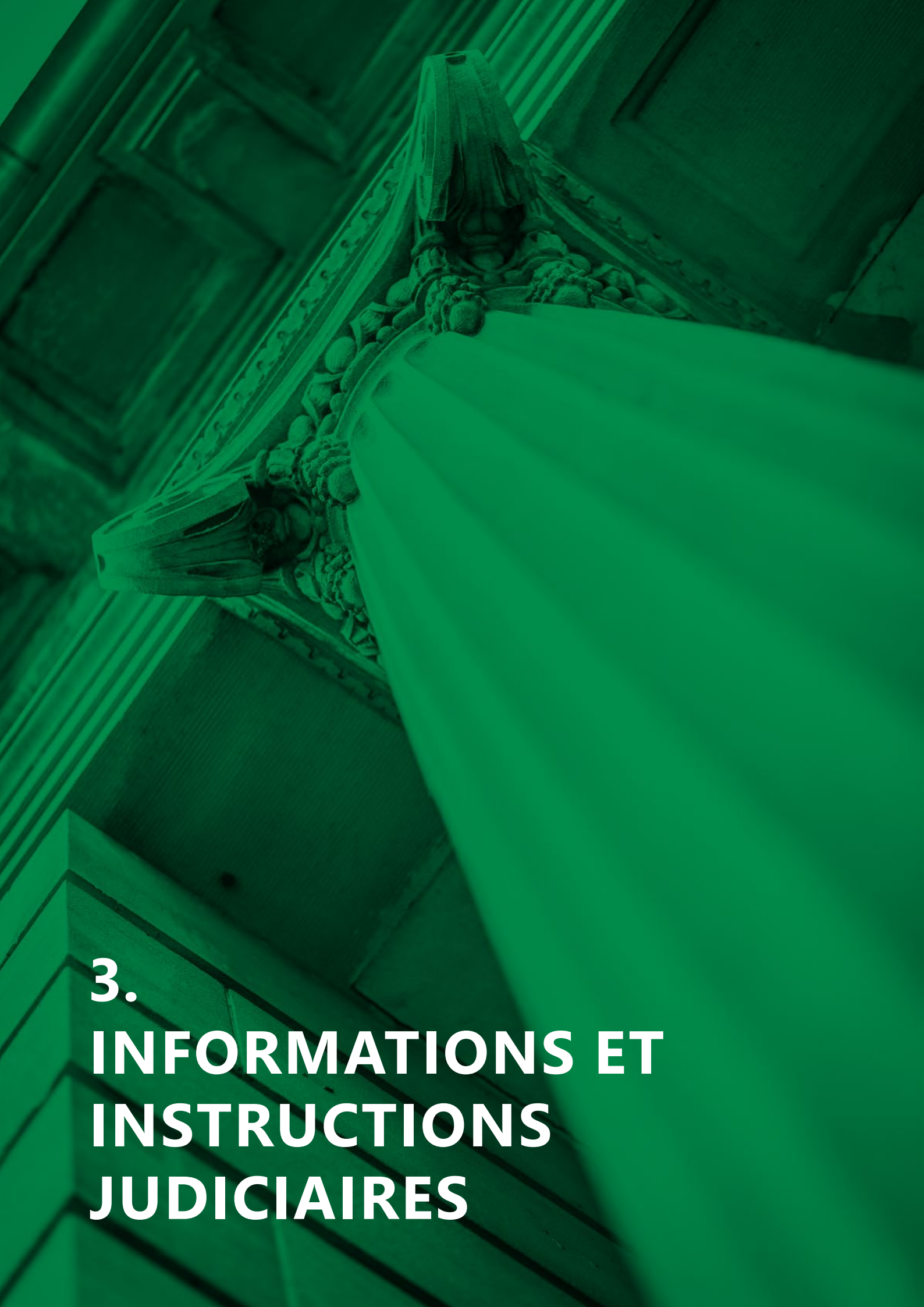
43 plaintes traitées ont pu être clôturées en 2023, 12 plaintes étaient toujours en cours de traitement début 2024. Par rapport aux années précédentes, on observe une légère diminution du nombre de plaintes recevables soumises au Comité permanent R. L'aperçu des services concernés par les plaintes déposées en 2023 indique une majorité de plaintes concernant la VSSE.

Services concernés par les plaintes introduites en 2023



Plaintes recevables





3. INFORMATIONS ET INSTRUCTIONS JUDICIAIRES

INFORMATIONS ET INSTRUCTIONS JUDICIAIRES

Sur ordre des autorités judiciaires, le Service d'Enquêtes R du Comité permanent R effectue également des enquêtes sur les membres des services de renseignement et de sécurité et de l'OCAM suspectés d'avoir commis un crime et/ou un délit (art. 40, alinéa 3 L.Contrôle).

Lorsqu'ils remplissent une mission de police judiciaire, les membres du Service d'Enquêtes R ne sont plus soumis à l'autorité du Comité permanent R mais à celle du procureur général près la cour d'appel ou du procureur fédéral (art. 39 L.Contrôle). Le président du Comité doit cependant veiller à ce que l'exécution des missions de police judiciaire n'entrave pas l'exécution des autres missions légales du Comité.

Durant l'année 2023, le Service d'enquêtes R s'est vu confier la gestion de trois enquêtes à la suite de plaintes contre « X » déposées par la Sûreté de l'Etat pour des faits présumés de violation de secret professionnel en son sein. Ces enquêtes étaient toujours en cours au 31 décembre 2023. À la clôture d'une enquête judiciaire, le Service d'enquêtes R communique un rapport d'information au Président du Comité permanent R si cette enquête fait apparaître un manque d'efficacité au sein des services de renseignement, une coordination insuffisante entre ces services ou une atteinte par ces mêmes services aux droits que la Constitution et la loi confèrent aux personnes. En 2023, aucune enquête n'a abouti à de tels constats.

4. MÉTHODES (PARTICULIÈRES) DE RENSEIGNEMENT

MÉTHODES (PARTICULIÈRES) DE RENSEIGNEMENT

Les méthodes exécutées par le SGRS

Le Comité est chargé du contrôle *a posteriori* des méthodes particulières de renseignement. Ce contrôle porte sur la légalité, la proportionnalité et la subsidiarité de ces méthodes.

Pour l'année 2023, le Comité s'est (pour la première fois) basé sur les chiffres fournis par les services de renseignement eux-mêmes. Ainsi, entre le 1er janvier et le 31 décembre 2023, 669 autorisations ont été émises par le SGRS pour l'utilisation de méthodes particulières de renseignement (dont 448 spécifiques et 221 exceptionnelles).

Les tableaux et graphiques ci-dessous détaillent les méthodes exécutées par le SGRS au cours de l'année 2023.

Méthodes spécifiques (SGRS)	2023
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)	22
Accès en temps réel aux images de caméras de police de lieux accessibles au public (18/4 §3 L.R&S)	14
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
S'infiltrer dans le monde virtuel sous couvert d'un faux nom ou d'une fausse qualité (art. 18/5/1 L.R&S)	0
Prendre connaissance des données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art. 18/6 L.R&S)	0
Requérir le concours d'un fournisseur privé de service en matière de transport ou de voyage afin d'obtenir les données de transport et de voyage (art. 18/6/1 L.R&S)	0
Identifier, à l'aide d'un moyen technique, les services et moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée (art. 18/7 § 1er, 1° L.R&S)	12
Requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, au moyen de paiement et au moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 § 1er, 2° L.R&S)	0
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 § 1er, 1° L.R&S)	202
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 § 1er, 2° L.R&S)	198
TOTAL	**448**

Méthodes exceptionnelles (SGRS)	2023
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)	15
Accès en temps réel aux images de caméras de police de lieux non accessibles au public (18/11 §3 L.R&S)	4
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)	14
S'infiltrer dans le monde réel (art. 18/12/1 L.R&S)	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	6
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	14
S'introduire dans un système informatique (article 18/16 L.R&S)	40
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	128
TOTAL	**221**

En 2023, le SGRS constate une augmentation considérable des autorisations de méthodes spécifiques. En particulier, le recours aux données de localisation d'un trafic de communications électroniques a connu une nette augmentation.

Le service de renseignement militaire fait également état d'une augmentation des méthodes exceptionnelles, confirmant la tendance dessinée en 2022. Tout comme en 2022, les intrusions informatiques (art. 18/16 L.R&S) et les écoutes téléphoniques (art. 18/17 L.R&S) sont les méthodes les plus utilisées et qui ont connu la plus forte augmentation.

En 2023, l'une des priorités du SGRS était l'espionnage, notamment à travers le suivi des attachés de défense ou diplomates étrangers accrédités pour la Belgique, l'Union européenne ou l'OTAN. Le suivi de l'extrémisme au sein des forces armées constitue également un point d'attention du service. Enfin, la criminalité organisée et les menaces à l'encontre des infrastructures et du personnel militaires ont fait l'objet d'un suivi spécifique par le SGRS.

Les méthodes ordinaires 'plus'

À l'origine, les méthodes ordinaires de renseignement étaient uniquement soumises au contrôle régulier du Comité. Toutefois, depuis plusieurs années, la Loi sur le renseignement prévoit des méthodes ordinaires pour lesquelles le Comité est chargé d'une mission de contrôle particulière et/ou pour lesquelles le service de renseignement concerné se voit imposer une obligation supplémentaire de fournir des informations au Comité (ce que l'on appelle les 'méthodes ordinaires plus'). L'obligation de contrôle ou d'information est réglementée différemment pour chacune de ces méthodes, et ce, malgré le plaidoyer du Comité en faveur d'une uniformisation de cette obligation.

Méthodes ordinaires 'plus' (SGRS)	2023
Identification de l''abonné ou de l'utilisateur habituel' de télécommunications (art. 16/2 L.R&S)	509
Recherches ciblées de données PNR (art. 16/3 L.R&S)	51
Utilisation d'images de caméras de police (art. 16/4, §2 L.R&S)	40
Réquisition de certaines données financières (art. 16/6 L.R&S)	38

Les statistiques relatives aux demandes d'accès aux données des passagers (*Passenger Name Records* (PNR)) par le SGRS s'arrêtent au 13 octobre 2023. En effet, l'arrêt de la Cour constitutionnelle du 12 octobre 2023 (arrêt 131/2023) a annulé l'article 16/3 L.R&S. A la suite d'une question préjudicielle posée à la Cour de Justice de l'Union européenne, la Cour a estimé que le champ d'application pour les services de renseignement était beaucoup plus large que ce que prévoyait initialement la réglementation européenne et que l'absence de contrôle indépendant préalable des demandes des services de renseignement constitue une violation des droits des citoyens. Pour cette raison, plusieurs articles de la loi du 25 décembre 2016 relative au traitement des données des passagers ont été supprimés, ainsi que l'article 16/3 L.R&S qui réglementait cette demande d'accès. Par conséquent, le SGRS ne peut plus interroger la banque de données PNR. Le législateur s'est engagé à résoudre ce problème dès que possible par une loi de réparation tenant compte des préoccupations de la Cour.

Les méthodes exécutées par la VSSE

Pour l'année 2023, le Comité s'est (pour la première fois) basé sur les chiffres fournis par les services de renseignement eux-mêmes. Ainsi, entre le 1er janvier et le 31 décembre 2023, 1 718 autorisations ont été émises par la VSSE pour l'utilisation de méthodes particulières de renseignement (dont 1 369 spécifiques et 349 exceptionnelles). Il convient de noter que la VSSE comptabilise les MRD par opération, tandis que le SGRS comptabilise les MRD par article de loi concerné. C'est pourquoi, une comparaison entre les chiffres des deux services n'est pas souhaitable.

Les tableaux et graphiques ci-dessous détaillent les méthodes exécutées par la VSSE au cours de l'année 2023.

Méthodes spécifiques (VSSE)	2023
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)	142
Accès direct aux images de caméras de police de lieux accessibles au public (18/4 §3 L.R&S)	0
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
S'infiltrer dans le monde virtuel sous couvert d'un faux nom ou d'une fausse qualité (art. 18/5/1 L.R&S)	0
Prendre connaissance des données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art. 18/6 L.R&S)	0
Requérir le concours d'un fournisseur privé de service en matière de transport ou de voyage afin d'obtenir les données de transport et de voyage (art. 18/6/1 L.R&S)	23
Identifier, à l'aide d'un moyen technique, les services et moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée (art. 18/7 § 1er, 1° L.R&S)	50
Requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, au moyen de paiement et au moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 § 1er, 2° L.R&S)	0
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 § 1er, 1° L.R&S)	577
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 § 1er, 2° L.R&S)	577
TOTAL	**1369**

Méthodes exceptionnelles (VSSE)	2023
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)	5
Accès en temps réel aux images de caméras de police de lieux non accessibles au public (18/11 §3 L.R&S)	0
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)	26
S'infiltrer dans le monde réel (art. 18/12/1 L.R&S)	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	25
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	45
S'introduire dans un système informatique (article 18/16 L.R&S)	65
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	183
TOTAL	**349**

Comme pour le SGRS, la VSSE constate une forte augmentation du nombre de méthodes spécifiques, en particulier la prise de connaissance des données de localisation d'un trafic de communications électroniques. Cette augmentation s'explique notamment par l'augmentation parallèle des membres du personnel de la Sûreté de l'Etat, ce qui permet de traiter davantage de dossiers de menace et donc d'exécuter davantage de méthodes.

Pour ce qui est des méthodes exceptionnelles, le service fait part, comme le SGRS, d'un recours croissant aux intrusions dans des systèmes informatiques (art. 18/16 L.R&S) et aux écoutes téléphoniques (art. 18/17 L.R&S). Par contre, la VSSE fait état d'une diminution notable du nombre d'observations de lieux non accessibles au public.

Parmi les menaces suivies par le service de renseignement civil, le terrorisme djihadiste et l'espionnage sont prioritaires. En effet, la VSSE s'intéresse notamment aux réseaux terroristes en ligne et aux loups solitaires et suit attentivement les conflits géopolitiques en Asie centrale et au Moyen orient ainsi que les menaces contre certains pays européens tels la Suède et ses ressortissants. En matière d'espionnage, avec quelques pays qui sont suivis principalement comme la Russie, la Chine ou l'Iran. Ainsi, le suivi de la VSSE s'est intensifié depuis l'invasion de l'Ukraine et vise particulièrement les agents des services de renseignement russes travaillant sous couvertures diplomatiques. Il en va de même pour les services de renseignement chinois et leurs tentatives d'influence au sein des universités ou même parmi les responsables politiques.

A côté de ces deux menaces principales, la VSSE suit également attentivement les menaces d'ingérence et d'extrémisme. Ainsi, bien avant le Qatargate, la VSSE suivait déjà un certain nombre d'agents d'influence. À la suite de la juridicisation de ce dossier, la VSSE a continué à investir dans le suivi de la menace d'ingérence. Depuis 2022, la VSSE a également réinvesti la menace de la criminalité organisée, plus particulièrement les menaces vis-à-vis de nos institutions étatiques, services publics tels que les services de police, les douanes ou la magistrature mais également les menaces à l'encontre du monde politique.

Les méthodes ordinaires 'plus'

À l'origine, les méthodes ordinaires de renseignement étaient uniquement soumises au contrôle régulier du Comité. Toutefois, depuis plusieurs années, la Loi sur le renseignement prévoit des méthodes ordinaires pour lesquelles le Comité est chargé d'une mission de contrôle particulière et/ou pour lesquelles le service de renseignement concerné se voit imposer une obligation supplémentaire de fournir des informations au Comité (ce que l'on appelle les 'méthodes ordinaires plus'). L'obligation de contrôle ou d'information est réglementée différemment pour chacune de ces méthodes, et ce, malgré le plaidoyer du Comité en faveur d'une uniformisation de cette obligation.

Méthodes ordinaires 'plus' (VSSE)	2023
Identification de l'abonné ou de l'utilisateur habituel' de télécommunications (art. 16/2 L.R&S)	4417
Recherches ciblées de données PNR (art. 16/3 L.R&S)	318
Utilisation d'images de caméras de police (art. 16/4, §2 L.R&S)	51
Réquisition de certaines données financières (art. 16/6 L.R&S)	135

Les statistiques relatives aux demandes d'accès aux données des passagers (*Passenger Name Records* (PNR)) par la VSSE s'arrêtent au 13 octobre 2023. En effet, l'arrêt de la Cour constitutionnelle du 12 octobre 2023 (arrêt 131/2023) a annulé l'article 16/3 L.R&S. A la suite d'une question préjudicielle posée à la Cour de Justice de l'Union européenne, la Cour a estimé que le champ d'application pour les services de renseignement était beaucoup plus large que ce que prévoyait initialement la réglementation européenne et que l'absence de contrôle indépendant préalable des demandes des services de renseignement constitue une violation des droits des citoyens. Pour cette raison, plusieurs articles de la loi du 25 décembre 2016 relative au traitement des données des passagers ont été supprimés, ainsi que l'article 16/3 L.R&S qui réglementait cette demande d'accès. Par conséquent, la VSSE ne peut plus interroger la banque de données PNR. Le législateur s'est engagé à résoudre ce problème dès que possible par une loi de réparation tenant compte des préoccupations de la Cour.

Contrôle *a posteriori*

Le Comité permanent R est chargé du contrôle *a posteriori* de la mise en œuvre des méthodes de renseignement spécifiques et exceptionnelles. Le Comité soumet *toutes* les autorisations de ces méthodes à une enquête *prima facie*, et ce, en vue de décider d'une éventuelle saisine (art. 43/4 L.R&S). Le Comité peut être saisi de cinq manières : d'initiative, à la demande de l'Autorité de protection des données, à la suite d'un dépôt de plainte par un citoyen, à la suite de la suspension d'une méthode spécifique ou exceptionnelle pour cause d'illégalité et à l'interdiction de l'exploitation des données par la Commission BIM ou quand le ministre compétent a donné son autorisation sur la base de l'article 18/10, § 3 L.R&S.

Par ailleurs, le Comité peut également être saisi en sa qualité d''auteur 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 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	2022	2023
1. D'initiative	16	12	16	3	1	1	4	2	1	5	0
2. Autorité de protection des données	0	0	0	0	0	0	0	0	0	0	0
3. Plainte	0	0	0	1	0	0	0	0	0	0	0
4. Interdiction d'exploitation par la Commission BIM	5	5	11	19	15	10	12	9	8	9	13
5. Autorisation du ministre	2	1	0	0	0	0	0	0	0	0	0
6. Auteur d'avis préjudiciel	0	0	0	0	0	0	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**	**11**	**9**	**14**	**13**

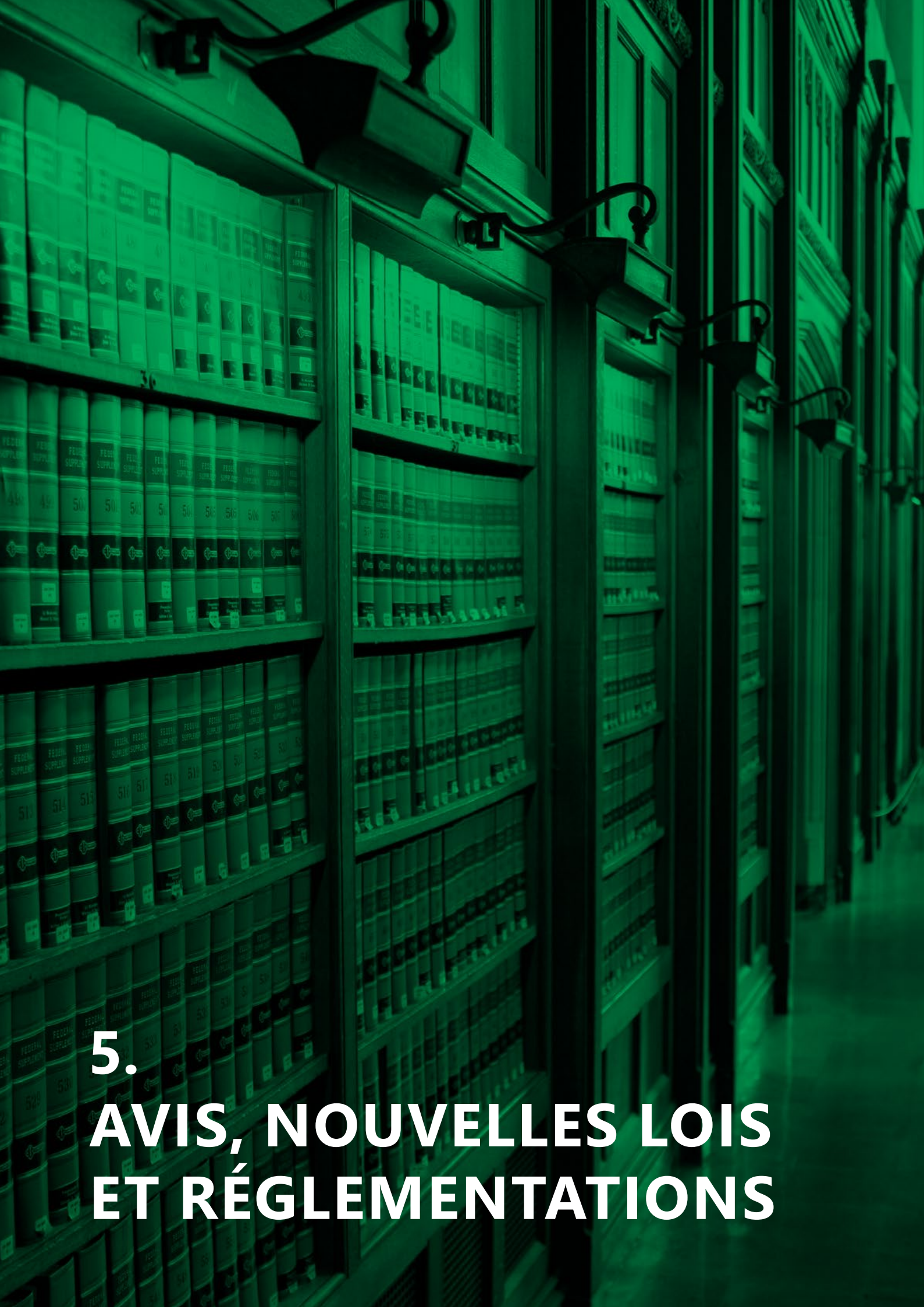
Le nombre de décisions prises par le Comité est resté stable en 2023. Elles étaient toutes le résultat d'une suspension ordonnée par la Commission BIM. Une fois saisi, le Comité peut prendre plusieurs types de décisions (intermédiaires). Dans dix cas, il a été décidé de mettre fin à la méthode ; dans trois autres cas, le Comité a décidé d'une cessation partielle de la méthode, permettant aux services d'utiliser une partie seulement des informations recueillies.

Interceptions à l'étranger, prises d'images et intrusions dans des systèmes informatiques

L'article 44 de la L.R&S permet au Service Général du Renseignement et de la Sécurité de rechercher, capter, écouter, prendre connaissance et enregistrer toute forme de communications émises ou reçues à l'étranger. Ainsi, l'intrusion dans un système informatique (art. 44/1 L.R&S) et la prise d'images fixes ou animées à l'étranger (art. 44/2 L.R&S) font également partie des possibilités d'action du service de renseignement militaire. Le Comité permanent R réalise un contrôle préalablement à, pendant et après l'exécution de ces méthodes.

Les plans relatifs aux interceptions, aux intrusions et aux prises d'images pour l'année 2023 ont été remis au Comité permanent R dans le courant du mois de janvier 2023. Ces plans respectent les prescrits légaux. Fin 2023, le Comité permanent R a également visité 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 pu constater qu'il avait été tenu compte des quelques remarques formulées en 2021. Une inspection a également été réalisée sur le site du service, au sein du SGRS, en charge de l'exécution du plan d'intrusion. À cette occasion, il a pu constater les importants investissements en cours et déjà réalisés afin d'être en mesure d'exécuter les missions planifiées.

En ce qui concerne le contrôle après l'exécution des interceptions, intrusions ou prises d'images, le Comité permanent R a reçu l'ensemble des listes légalement prévues. Le Comité ne peut toutefois pas communiquer davantage à cet égard, étant donné le caractère classifié de cette matière.



5.
AVIS, NOUVELLES LOIS ET RÉGLEMENTATIONS

AVIS, NOUVELLES LOIS ET RÉGLEMENTATIONS

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 les orientations politiques des ministres compétents, exclusivement à la demande de la Chambre des représentants ou du Ministre compétent (art. 33 L.Contrôle). Par ailleurs, le Comité doit rendre des avis en tant qu'Autorité de contrôle compétente dans le cadre des traitements de données à caractère personnel (artt. 73 et 95 LPD) 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.). Il arrive que des avis soient formulés à partir d'une double compétence.

Au cours des dernières années, le Comité est de plus en plus souvent sollicité pour rendre un avis ; le temps consacré à cette mission a considérablement augmenté. En 2023, le Comité a été sollicité à onze reprises : par le ministre de la Justice à quatre reprises (dont une demande d'avis a été soumise au Comité par l'intermédiaire de l'Autorité de protection des données (APD)) et par la ministre de l'Intérieur à sept reprises. La plupart des demandes d'avis portaient sur des avant-projets de loi, trois d'entre elles concernaient un projet d'arrêté royal et une demande visait un projet d'arrêté ministériel. Les thèmes étaient variés, allant de la recherche privée à la reconnaissance du bouddhisme, en passant par un nouveau Code de la navigation. Le délai moyen pour rendre un avis est de trois mois. Tous les avis sont consultables dans leur intégralité sur le site internet du Comité permanent R.

La recherche privée

L'exercice des activités de recherche privée était régi par une loi datant de 1991. Cette loi était devenue obsolète et ne tenait pas compte des nouvelles règles de droit, des nouvelles pratiques et possibilités d'enquête. Par le passé (en octobre 2017), une loi réglementant la sécurité privée et particulière a été publiée. Un nouvel avant-projet de loi prévoyait désormais une révision intégrale de la recherche privée. Ainsi, les entreprises proposant ces services doivent être titulaires d'une autorisation et plusieurs conditions de sécurité et de formation s'imposent aux membres de leur personnel. En outre, l'avant-projet mettait l'accent sur le contrôle proactif sous la forme de systèmes d'autorisation lié à un screening pour le personnel, ainsi que sur le contrôle réactif du respect de la loi. Le gouvernement entend ainsi garantir la fiabilité et la qualité des services et le respect de l'État de droit. L'avant-projet a été soumis pour avis, entre autres, au Comité permanent R étant donné qu'un traitement de données à caractère personnel par les deux services de renseignement et de sécurité était prévu. Dans son avis, le Comité saluait le retour d'un régime de screening uniforme pour tous les acteurs du secteur de la sécurité privée. Néanmoins, il regrettait la coexistence de plusieurs types de screenings (habilitation de sécurité, vérification de sécurité, enquête sur les conditions de sécurité, enquête d'intégrité…) et ce, alors que la finalité sous-jacente de ces screenings ne diffère que très peu.

Toutefois, compte tenu des modifications apportées par le nouveau projet de loi soumis au Comité, une nouvelle différence risque d'apparaitre entre les réglementations relatives à la surveillance privée, d'une part, et à la recherche privée, d'autre part. Dans son deuxième avis, le Comité a estimé que la finalité du screening n'était pas claire et que le cadre d'évaluation devait être déterminé de manière beaucoup plus précise.

L'accès direct à la Banque de données Nationale Générale

En 2019, la loi sur la fonction de police a été modifiée pour permettre aux services de renseignement d'accéder à la Banque de données Nationale Générale (BNG). Un projet d'arrêté royal en précisait les modalités d'exécution. Concrètement, les catégories de données à caractère personnel auxquelles les services de renseignement auront directement accès ainsi que la méthode d'accès ont été définies. Dans son avis, le Comité demandait des clarifications concernant la notion et le champ d'application de cet « accès direct », l'accès aux données médicales ainsi que la motivation des consultations et de l'obligation d'enregistrement. Les traitements ultérieurs des données de la BNG (par exemple, le transfert de données), la journalisation des traitements et l'exportation des données de la BNG vers les fichiers de la VSSE et du SGRS soulevaient également plusieurs questions. Enfin, l'accent a été mis sur la réciprocité en matière d'échange de données. Cette réciprocité n'exige pas que les services de police aient également un accès direct aux banques de données des services de renseignement. Au contraire, le législateur a semblé supposer que le régime juridique actuel, à condition d'une applica-

tion effective, impliquait déjà la réciprocité.

Par la suite, un projet d'arrêté ministériel relatif à l'accès direct des services de renseignement et de sécurité à la BNG a été soumis au Comité. Celui-ci a formulé dans un deuxième avis des observations sur la méthode de classification et sur la distinction entre les informations judiciaires et les données de police administrative. Le Comité s'est également interrogé sur la pertinence de règles différenciées, qui allaient compliquer l'exécution et le contrôle de ces dispositions.

Le bouddhisme en tant qu'organisation philosophique non confessionnelle

Un avant-projet de loi visait à reconnaître le bouddhisme en tant qu'organisation philosophique non confessionnelle sur la base de l'article 181 §2 de la Constitution, à reconnaître l'Union Bouddhiste de Belgique comme organe représentatif de cette communauté en Belgique ainsi qu'à organiser le fonctionnement des communautés bouddhistes locales et la fonction des délégués bouddhistes. L'avant-projet prévoyait l'introduction d'un nouveau traitement de données à caractère personnel par les services de renseignement et l'Organe de Coordination pour l'Analyse de la Menace (OCAM). Le Comité a estimé que l'avant-projet devait être complété en de nombreux points afin que la portée du screening qu'il met en place soit précisée dans la loi.

La banque de données commune 'TER'

Fin mars 2023, le Conseil des ministres a approuvé un projet de loi et un projet d'arrêté royal relatifs au fonctionnement de la banque de données commune Terrorisme, Extrémisme, processus de Radicalisation (BDC TER). Le projet vise à transposer dans une loi autonome les dispositions de la Loi sur la fonction de police relatives aux banques de données communes 'Terrorist fighters' et Propagandistes de haine'. Ce faisant, il entérine le fait qu'il n'y a qu'une seule banque de données commune pour traiter les matières de terrorisme, d'extrémisme et de radicalisme (BDC TER).

Créée après les attentats de 2016, cette banque de données rassemble les informations sur des personnes perçus comme extrémistes et les terroristes suivis en Belgique dans le cadre de la « Stratégie TER »et permet aux services de renseignement et de sécurité de partager des informations et de déterminer quel service est le mieux placé pour prendre quelle(s) mesure(s). L'OCAM, la VSSE, le SGRS, le ministère public, la police intégrée, le Centre de crise, l'Office des Etrangers, entre autres, ont un rôle à jouer et certaines obligations à remplir à cet égard. Par ces projets de loi et d'arrêté royal, les ministres de la Justice et de l'Intérieur souhaitent améliorer le fonctionnement des banques de données communes et la structure de sécurité qui les entoure.

En sa qualité d'autorité de contrôle compétente, le Comité a formulé une série de remarques sur les objectifs du traitement des données à caractère personnel, sur les règles applicables en matière de protection des données, sur le « *need to know* » (besoin d'en connaitre) pour l›accès aux ou pour la consultation des données à caractère personnel, mais également sur la durée de conservation des données, sur les journalisations, sur l'interconnexion avec d'autres banques de données, sur la communication de données de la BDC TER à des autorités ou institutions tierces, ou encore sur l'obligation, pour les services de renseignement, d'alimenter cette banque de données commune.

La fiabilité des personnes dans le secteur nucléaire civil

Un avant-projet de loi modifiait le régime des attestations de sécurité pour le secteur nucléaire. Le texte visait à revoir le régime de contrôle de fiabilité des personnes dans le secteur nucléaire en vue de davantage de souplesse et d'efficacité. A cette fin, il a été décidé d'étendre la dérogation prévue pour le secteur nucléaire à l'article 8*bis* de la Loi Classification.

Le Comité n'a pu que constater que cette option rend labyrinthique un système déjà très complexe de contrôle de fiabilité des personnes. Il a invité les auteurs du projet à analyser la nécessité d'emprunter cette voie pour répondre à la finalité poursuivie. Par ailleurs, le projet, qui vise à fournir une base légale pour le contrôle de fiabilité des personnes pour l'accès à des éléments non catégorisés du secteur nucléaire et radiologique, proposait d'insérer une nouvelle forme d'attestation de sécurité. Pourtant, rien ne permet d'expliquer les raisons pour lesquelles le régime existant pour les autres secteurs (avis de sécurité et certificats de sécurité, prévus respectivement à l'art 22*quinquies*, art 22*quinquies*/1 W.C&VM et art 22*bis*, deuxième alinéa, W.C&VM) ne pourrait pas répondre à la finalité poursuivie. Une fois de plus, ce choix ne fait que compliquer un système de vérification de la fiabilité des personnes. Dans son avis, il invitait les auteurs du projet à analyser la nécessité d'emprunter cette voie au regard des finalités poursuivies et à justifier les choix opérés.

La consultation du système ETIAS

L'ETIAS est le nouveau système d'information et d'autorisation de voyage de l'Union européenne. Ce système s'applique aux ressortissants de pays tiers exemptés de visa qui souhaitent se rendre dans l'espace Schengen. Ces ressortissants doivent remplir un formulaire en ligne avant leur voyage dans l'espace Schengen pour obtenir une autorisation de voyage. L'introduction de l'ETIAS vise à renforcer la sécurité intérieure, à prévenir l'immigration clandestine et à protéger la santé publique. L'objectif est d'identifier les personnes qui peuvent représenter un risque pour la sécurité ou l'immigration avant même leur départ pour l'UE. L'avant-projet prévoyait que des agents détachés de la VSSE et du SGRS feraient partie d'une section hébergée au Centre de crise National, compétente pour « traiter les réponses positives relatives aux risques en matière de sécurité et aux risques épidémiques élevés ». L'avant-projet élargit toutefois le champ d'application du règlement européen en autorisant les deux services de renseignement belges à utiliser le système ETIAS pour toutes les menaces qu'ils ont l'obligation de suivre. Or, le règlement ETIAS limite les consultations et l'inscription sur une liste de surveillance aux personnes susceptibles d'être liées à des « infractions terroristes ou à d'autres infractions pénales graves ». Le Comité a estimé qu'en donnant aux services de renseignement une possibilité de consultation générale et en leur permettant d'inscrire sur la liste de surveillance des personnes qui ne relèvent pas de la finalité du système ETIAS, le règlement n'est pas correctement appliqué.

Digitalisation de la Justice

En juillet 2023, le Conseil des ministres a approuvé un avant-projet de loi sur la digitalisation de la Justice qui modifiait plusieurs lois relevant de la compétence du ministère de la Justice. Il s'agissait notamment du cadre légal pour la conservation des casiers judiciaires dans un registre central, de la durée de conservation des données de vote électronique ou de l'enregistrement des empreintes digitales dans le Système européen d'information sur les casiers judiciaires. En ce qui concerne plus particulièrement les services de renseignement, le projet visait à étendre la définition d'officier des méthodes (chargé de contrôler l'utilisation des méthodes particulières de renseignement) afin de permettre à un plus grand nombre de membres du personnel de postuler à ce poste. Dans son avis, le Comité soulignait l'importance d'une formation spécifique pour le personnel chargé du contrôle, en interne, des conditions de mise en œuvre et d'exécution des méthodes particulières de renseignement. Le Comité suggérait également que toute nomination d'un officier des méthodes par l'administrateur général de la VSSE ou le chef du SGRS se fasse après avis de la Commission BIM.

L'intégration de l'Autorité Nationale de Sécurité au sein de la VSSE

Jusqu'à la fin de l'année 2023, l'Autorité nationale de sécurité (ANS) était un organe collégial, dont la VSSE et le SGRS faisaient partie, logé au sein du SPF Affaires étrangères. Par la loi du 7 avril 2023, les compétences de l'ANS ont été réparties entre la Police fédérale, désormais responsable de la délivrance et du retrait des avis de sécurité, et l'ANS, chargée de la délivrance et du retrait des habilitations de sécurité ainsi que du contrôle des normes de sécurité applicables au traitement et à la conservation des informations classifiées. Depuis le 1er janvier 2024, l'ANS fait partie de la VSSE en tant qu'entité autonome. Dans ce cadre, trois projets d'arrêtés royaux définissant le fonctionnement et l'organisation de cette autorité de sécurité ont été soumis au Comité pour avis. Le Comité s'est notamment interrogé sur le pouvoir de délégation de l'Administrateur général de la VSSE.

Plans de sûreté portuaire et le rôle des services de renseignement

En septembre 2023, le Comité a été invité, en sa qualité d'Autorité de contrôle compétente, à rendre un avis sur le projet de loi modifiant le Code belge de la navigation. L'objectif principal de cette modification est d'améliorer la sûreté maritime en Belgique face à l'augmentation de la criminalité liée aux drogues dans et autour des zones portuaires. Il s'agit notamment de dispositions relatives à l'extension du champ d'application de la surveillance, à des contrôles supplémentaires, à l'introduction de vérifications de sécurité pour certaines fonctions, à la politique d'intégrité et à la réglementation des caméras. Les services de renseignement sont concernés par les règles relatives à l'installation et à l'utilisation de caméras dans les installations portuaires et dans les ports par la capitainerie. Ils interviennent notamment dans la décision d'installer des caméras (intelligentes) dans les ports. Le projet précisait également les modalités d'accès par les services de renseignement aux images et aux enregistrements sonores des caméras. Sur ce dernier point, le Comité appelait à régler de manière uniforme, dans la loi organique des services de renseignement, leur accès aux informations et images des caméras.

Nouvelles lois et réglementations

En 2023, de nombreuses lois et réglementations ont été modifiées en ce qui concerne le fonctionnement, les compétences et le contrôle des services de renseignement et de sécurité et le travail de renseignement.

Dès le début du mois de janvier 2023, la *Loi du 8 décembre 2022 relative aux canaux de signalement et à la protection des auteurs de signalement d'atteintes à l'intégrité dans les organismes du secteur public fédéral et au sein de la police intégrée (MB 23 décembre 2022)* est entrée en vigueur. Le système de signalement mis en place comporte désormais trois options : le signalement interne, le signalement externe et la divulgation publique. Le canal de signalement externe pour les atteintes à l'intégrité au sein des organismes du secteur public fédéral a été institué auprès des médiateurs fédéraux. Des exceptions ont toutefois été prévues. Ainsi, le législateur a désigné le Comité permanent R comme canal de signalement externe chargé de recevoir et d'assurer le suivi des signalements d'atteintes à l'intégrité au sein de la VSSE et du SGRS. Il s'agit donc d'une tâche supplémentaire pour le Comité permanent R qui est désormais compétent, en tant que canal de signalement externe, pour informer sur le contenu et l'application de la loi, pour recevoir et assurer le suivi des signalements sur les atteintes à l'intégrité, mais aussi pour offrir une protection contre les représailles. La loi se base sur une définition spécifique de l'atteinte à l'intégrité ; par exemple, le harcèlement moral, la violence et le harcèlement sexuel au travail, ainsi que les violations des lois sur la discrimination, n'entrent pas dans le champ d'application de la loi sur les lanceurs d'alerte.

Le 14 février 2023, la *Loi portant assentiment de l'accord de coopération du 30 novembre 2022 entre l'État fédéral, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire française et la Commission communautaire commune visant à instaurer un mécanisme de filtrage des investissements directs étrangers (MB 7 juin 2024)* a été votée. Cela a permis la création d›un Comité de Filtrage Interfédéral de filtrage (CFI) des investissements étrangers. La tâche principale du CFI est d›analyser les investissements directs en provenance de pays tiers (par l›intermédiaire d›une société de l›Union européenne ou non) qui acquièrent un certain pourcentage des droits de vote dans une entreprise établie en Belgique, et de vérifier si ces investissements présentent des risques potentiels pour la sécurité nationale et les intérêts stratégiques. Le CFI peut ainsi identifier les menaces potentielles et prendre des mesures préventives pour protéger les secteurs nationaux sensibles, tels que les infrastructures et technologies critiques, les matières premières, l›énergie ou encore la défense. Depuis le 1er juillet 2023, le VSSE joue également un rôle important dans le contrôle des investissements directs étrangers dans les secteurs critiques. En effet, un accord de coopération prévoit que le Comité de coordination du renseignement et de la sécurité (CCRS) soit consulté pour chaque investissement examiné par le CFI. La Sûreté de l›État est chargée de vérifier si les nouveaux investissements étrangers constituent une menace pour les intérêts qu'elle doit protéger.

Sur la base d'un avis du Centre pour la Cybersécurité Belgique (CCB) et des services de renseignement, le Conseil national de Sécurité a décidé via la *Circulaire n°716 du 17 mars 2023 – Interdiction temporaire d'utiliser l'application TikTok (MB 31 mars 2023)*, pour le personnel des autorités publiques fédérales, d'interdire l'installation et l'utilisation de l'application TikTok sur les appareils de service et a recommandé de ne pas l'installer sur les appareils personnels ayant accès aux réseaux internes des autorités fédérales. Le 14 septembre 2023, le Conseil national de Sécurité a décidé de prolonger de six mois l'application de la circulaire.

Le 7 avril 2023, l'*arrêté royal modifiant l'arrêté royal du 23 janvier 2012 relatif la passation des marchés publics et de certains marchés de travaux, de fournitures et de services dans les domaines de la défense et de la sécurité (MB 2 juin 2023)* a été approuvé. Cette modification a donné aux pouvoirs adjudicateurs et aux entreprises publiques qui passent des marchés publics de valeur limitée (≤30 000 €) dans le domaine de la défense et de la sécurité la même flexibilité que pour les marchés publics dans les secteurs classiques.

Le même jour a été approuvé l'*arrêté royal du 7 avril 2023 modifiant l'arrêté royal du 14 janvier 1994 portant statut de l'administrateur général et de l'administrateur général adjoint de la Sûreté de l'État et l'arrêté royal du 5 décembre 2006 relatif à l'administration générale et à la cellule d'appui de la Sûreté de l'État (MB 17 avril 2023)*. En cas d'absence d'au moins six mois de l'administrateur(rice) général(e) ou de son adjoint, il est désormais possible de désigner un remplaçant temporaire.

Le changement législatif le plus important pour

le secteur du renseignement est sans doute l'adoption de la *Loi du 7 avril 2023 portant modification de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (MB 9 juin 2023)*. Le législateur a jugé nécessaire de mettre les dispositions de la loi du 11 décembre 1998 sur la classification en conformité avec les obligations internationales en vigueur, notamment en matière de sécurité de l'information. L'Autorité nationale de sécurité se voit également attribuer des compétences supplémentaires et un cadre juridique est prévu pour le « service public réglementé » de Galileo, le système mondial de radionavigation par satellite de l'Union européenne.

Avec cette loi, le législateur prévoit un certain nombre d'adaptations afin que la communication dans un contexte international et, plus particulièrement, l'échange d'informations classifiées soient plus fluides, plus efficaces et plus uniformes. Ainsi, en plus des niveaux « confidentiel », « secret » et « très secret », un quatrième niveau de classification « restreint » est créé. Les mesures de protection minimales sont adaptées à ce nouveau niveau de classification. Ces mesures sont désormais réparties en cinq catégories, à savoir les mesures applicables lors de la gestion d'informations classifiées, les mesures de protection relatives aux personnes, les mesures de protection liées aux marchés publics, les mesures de protection physiques et les mesures de protection des systèmes d'information et de communication.

En fonction de tous ces changements, l'Autorité nationale de sécurité (ANS) se verra attribuer un certain nombre de compétences supplémentaires. Le législateur a également prévu d'emblée une nouvelle structure organisationnelle : l'ANS ne consistera plus en une coopération collégiale entre neuf services du secteur public fédéral avec un secrétariat logé au sein du SPF Affaires étrangères (*supra*), mais fera désormais partie de la Sûreté de l'État. L'ANS ne sera plus non plus responsable de la délivrance et du retrait des attestations de sécurité et de la délivrance des avis de sécurité. Ces compétences ont été transférées à la Police fédérale. Un arrêté d'exécution précisera cette nouvelle structure et organisation dans le courant de l'année 2024. Cependant, le législateur a déjà défini de nouvelles compétences. L'ANS sera notamment chargée de la préparation de la politique belge de sécurité relative à la protection des informations classifiées ; du contrôle de la mise en place des mesures de protection ; de la délivrance, de la modification, de la suspension et du retrait des habilitations de sécurité ; de la délivrance, de la modification, de la suspension et du retrait des approbations des installations physiques, des systèmes de communication et d'information et du matériel cryptographique.

Avec cette loi, le législateur a également (une fois encore) introduit un nouveau screening de sécurité : progressivement, tout le personnel militaire et civil du ministère de la Défense sera soumis à une vérification de sécurité au moins tous les cinq ans et devra disposer d'un avis de sécurité positif.

Le législateur a encore prévu la possibilité de percevoir une rétribution pour tous les agréments délivrés, tant pour le secteur privé que pour le secteur public, par l'ANS. Les articles 46 et 47 de la *Loi du 31 juillet 2023 visant à rendre la justice plus humaine, plus rapide et plus répressive IV (MB 9 août 2023)* prévoient ainsi que l'ANS, qui dépend désormais administrativement de la Sûreté de l'État, soit érigée en service administratif à comptabilité autonome pour la perception de ces rétributions.

L'*arrêté royal du 4 juin 2023 concernant la sûreté maritime (MB 26 juin 2023)* régit le fonctionnement de la Cellule de la Sûreté maritime, l'Autorité Nationale de Sûreté Maritime (ANSM) et les Comités locaux de la Sûreté Maritime au sein de la DG Navigation du SPF Mobilité et Transports. La Cellule de Sûreté maritime est responsable du fonctionnement et du suivi journaliers de ANSM, un organe de concertation présidé par le Directeur général de la DG Navigation. Cette autorité assure le suivi de la sûreté dans les ports et installations portuaires. Désormais, l'ANSM est composée du Directeur général de la DG Navigation, du Centre de crise national, de la VSSE, de l'Administration générale des Douanes et Accises, de la Défense, du SGRS, de l'OCAM et de la Police de la navigation.

À la suite de l'arrêt « La Quadrature du Net » (Cour de justice de l'Union européenne, 6 octobre 2020), de l'arrêt subséquent de la Cour constitutionnelle du 22 avril 2021 (arrêt n° 57/2021) et de l'arrêt de la même cour n° 58/2021 du 18 novembre 2021, le législateur a modifié, entre autres, la Loi du 13 juin 2005 relative aux communications électroniques par la loi du 20 juillet 2022 relative 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. En conséquence, le 13 octobre 2023, l'*arrêté royal du 4 octobre 2023 relatif à la conservation des données par les opérateurs de communications électroniques pour les autorités conformément aux articles 126 à 126/3 de la loi du 13 juin 2005 relative aux communications électroniques et aux statistiques sur la communication de ces données aux autorités* a été publié au

Moniteur belge.

Et le niveau européen n'est pas en reste. Avec la *Loi du 7 avril 2023 portant assentiment au Protocole additionnel à la Convention du Conseil de l'Europe pour la prévention du terrorisme, fait à Riga le 22 octobre 2015 (MB 24 mai 2023)*, ce Protocole additionnel, ratifié le 11 mai 2023, est entré en vigueur pour la Belgique le 1er septembre 2023. Il introduit de nouvelles infractions terroristes (par exemple, l'entraînement au terrorisme, (le financement) des voyages à l'étranger à des fins terroristes). Le protocole oblige également les États membres à prendre les mesures nécessaires pour assurer l'échange en temps utile de toutes les informations disponibles sur les personnes voyageant à l'étranger à des fins terroristes.

Le 20 septembre 2023 a été publiée au Journal officiel de l'Union européenne la *Décision d'exécution (UE) 2023/1795 de la Commission du 10 juillet 2023 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE-États-Unis*. La Commission y constate les modifications législatives apportées aux Etats-Unis qui rendent désormais possibles les transferts de données à caractère personnel depuis l'Union européenne vers certains organismes étasuniens.

Le 11 octobre 2023 était publié dans ce même Journal officiel le *Règlement (UE) 2023/2131 du Parlement européen et du Conseil du 4 octobre 2023 modifiant le Règlement (UE) 2018/1727 du Parlement européen et du Conseil et la Décision 2005/671/JAI du Conseil en ce qui concerne l'échange d'informations numériques dans les affaires de terrorisme*. Le règlement renforce entre autres les exigences concernant l'échange d'informations relatives aux enquêtes et poursuites pour infractions terroristes entre les autorités nationales et l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust).

De son côté, la *Loi du 12 février 2023 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 (MB 20 avril 2023)* réglemente le cadre général de la protection et de la sécurité des informations classifiées échangées entre les deux pays voisins.

Entre-temps, la ratification par la Belgique de la *Convention 108+* du Conseil de l'Europe se fait par contre attendre (voir *supra*). Cette convention est le premier instrument international qui traite spécifiquement de la sécurité nationale et donc des services de renseignement et de sécurité. Elle offre des garanties pour une collecte et un traitement prudents des données et établit des principes en matière d'examen et de contrôle indépendants. Récemment, le Parlement européen a adopté des recommandations soulignant l'importance de la Convention 108+ pour les États membres de l'Union européenne (P9_TA(2023)0244 du 15 juin 2023). Entre autres, le Parlement européen « *invite instamment tous les États membres à ratifier la convention sans plus tarder et à appliquer d'ores et déjà ses normes dans le droit national et à agir en conséquence en matière de sécurité nationale* » (paragraphe 47). De nombreux pays – en ce compris les voisins français le 27 mars 2023 – ont précédé la Belgique et ratifié la Convention. Le Comité permanent R préconise que la Belgique les rejoigne rapidement et transpose ainsi les normes de la Convention.

6.
CONTRÔLE DES BANQUES DE DONNÉES COMMUNES

CONTRÔLE DES BANQUES DE DONNÉES COMMUNES

En 2016, les ministres de l'Intérieur et de la Justice ont créé la banque de données commune *'foreign terrorist fighters'*. Cette banque de données commune a été modifiée en 2018 en banque de données commune *'terrorist fighters'* (BDC TF) pour inclure, 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 de la Loi sur la fonction de police (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.

La mission de contrôle

Pour le Rapport 2022, réalisé en 2023, le C.O.C. et le Comité permanent R ont décidé d'axer leur contrôle conjoint sur le suivi des recommandations antérieures et sur l'utilisation des banques de données communes par les services de sécurité et de renseignement. Le suivi des recommandations de l'enquête de contrôle du Comité permanent R relative à la radicalisation d'un militaire de la Défense réalisée en 2021 a également été intégré au contrôle.

Le contrôle a été annoncé aux services concernés, à savoir la Police fédérale, la Sureté de l'Etat (VSSE) et le Service général du renseignement et de la sécurité (SGRS) qui ont été interrogés par courrier. Les données de journalisation concernant les traitements effectués par les deux services de renseignement et de sécurité ont été fournies par la Police fédérale. Le rapport intégral est consultable sur le site web du Comité permanent R.

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, la création d'une éventuelle nouvelle banque de données commune doit préalablement être soumise à l'avis conjoint des Comité permanent R et au C.O.C. 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. 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. 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.

Suite au dossier du militaire radicalisé en 2021 et à l'attaque mortelle sur deux policiers à Schaerbeek, les ministres de la Justice et de l'Intérieur ont ordonné une analyse approfondie des interventions nécessaires pour améliorer le fonctionnement de la Banque de données commune et de la structure de sécurité qui l'entoure. Sur la base de cette analyse, les ministres ont élaboré un projet de loi et un projet d'arrêté royal[2] sur lesquels le COC et le Comité permanent R ont chacun rendu un avis (consultable sur le site du Comité permanent R).

2 Avant-projet de loi portant création de la banque de donnée commune « Terrorisme, Extrémisme, processus de Radicalisation (« T.E.R. ») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police et Projet d'arrêté royal relatif à la banque de données commune «Terrorisme, Extrémisme, processus de Radicalisation (« T.E.R. »).

7. FONCTIONNEMENT INTERNE

FONCTIONNEMENT INTERNE

Composition

La composition du Comité a changé en 2023 : Serge Lipszyc, premier substitut de l'auditeur du travail près l'auditorat du travail de Liège, a continué à remplir sa mission de Président et Thibaut Vandamme, substitut du procureur du Roi de l'arrondissement du Luxembourg, a poursuivi l'exercice de son mandat de conseiller. Le conseiller Pieter-Alexander De Brock a été remplacé le 28 mars 2023 par Linda Schweiger, conseillère générale à la Défense. Le Service d'enquêtes R est composé de six commissaires-auditeurs ; l'administration, dirigée par le greffier Frédéric Givron, compte quinze employés.

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 2023. En étaient membres avec voix délibérative Peter Buysrogge (N-VA), Yngvild Ingels (N-VA), Julie Chanson (Ecolo-Groen), 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 Boukili (PVDA-PTB), Tim Vandenput (Open Vld) et Meryame Kitir (Vooruit). La Présidente de la Chambre, Eliane Tillieux (PS), a assuré la présidence de la Commission. Georges Dallemagne (Les Engagés) a participé en tant que membre sans voix délibérative.

Dans le courant de l'année 2023, cinq réunions ont eu lieu à huis clos avec la Commission de suivi pour discuter des enquêtes de contrôle que le Comité permanent R avait clôturées et du fonctionnement interne du Comité.

Réunions communes avec le Comité permanent P

L'article 52 L.Contrôle prévoit qu'au minimum deux réunions se tiennent annuellement entre le Comité permanent R et le Comité permanent P. Au cours de l'année 2023, les réunions et interactions étaient fréquentes dans le cadre des enquêtes menées et des plaintes instruites conjointement par les Comités.

Budget

Le budget total approuvé par la Chambre des représentants pour 2023 était de 4 933 170 € et se composait de 3 317 000 € de dotation et de 1 616 170 € de boni 2022. Les frais de personnel représentent la majeure partie de ce budget (> 80%).

Digitalisation

Fin 2023, le Comité permanent R a obtenu de la Chambre des Représentants un budget spécifique en vue d'un projet de digitalisation d'envergure lui permettant de moderniser son fonctionnement. Il s'agit d'une étape décisive pour l'allègement des tâches administratives.

Synergies

Le Comité permanent R est et reste pleinement investi dans la recherche de synergies avec les autres institutions à dotation de la Chambre. En avril 2021, un accord avait en effet été trouvé au sein de la Commission de la Comptabilité sur les synergies à initier entre les institutions concernées. Les travaux se sont poursuivis en 2023. Ainsi, le Comité participe aux groupes de travail mis sur pied dans ce cadre (pilotage central des synergies, ICT, statuts harmonisés et marchés publics). Des résultats tangibles ont déjà été obtenus par la création d'un service partagé pour les voitures de service.

8. COOPÉRATION INTERNATIONALE

COOPÉRATION INTERNATIONALE

- 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 (initialement) cinq pays européens (la Belgique, le Danemark, les Pays-Bas, la Norvège et la Suisse) se concertent depuis plusieurs années afin de relever ces défis, en identifiant des méthodes de travail qui leur permettraient de limiter le risque de lacunes dans le contrôle *(International Oversight Working Group (IOWG))*. Depuis, le groupe s'est élargi à la Suède et à la Grande-Bretagne.

  En mai 2023, une réunion de l'IOWG s'est tenue au niveau du personnel *(staff meeting)* à La Haye. Après une brève présentation par les délégations des derniers développements intervenus au sein de leurs organes respectifs, les discussions ont principalement porté sur des thèmes variés allant du défi de la communication et de la transparence à la coopération technique en passant par la Convention 108+ et l'achat par les services de renseignements de jeux de données disponibles sur le marché *(commercially acquired datasets)*. Des préparatifs ont également été lancés en vue des réunions de novembre 2023.

  En novembre 2023 à Oslo, une réunion de l'IOWG a eu lieu, tant au niveau du personnel *(staff meeting)* que des dirigeants des différents organes de contrôle *(chair meeting)*. Après une brève présentation des derniers développements intervenus au sein de leurs juridictions et organes respectifs, l'agenda des domaines de discussions et échanges a été mis à jour. L'IOWG a décidé de travailler sur les priorités suivantes : (i) organiser des réunions plus techniques, éventuellement sous forme de *hackatons*, au sujet de l'intelligence artificielle ; (ii) renforcer l'utilisation de l'environnement numérique partagé de l'IOWG ; (iii) appréhender ensemble le défi de la communication et de la transparence dans le cadre d'un travail de contrôle d'activités essentiellement classifiées ; (iv) continuer les échanges en matière de coopération technique, sur le contrôle en général et sur certains sujets particuliers, comme l'achat par les services de renseignements de jeux de données disponibles sur le marché et la Convention 108+. Des préparatifs ont également été lancés en vue du « *staff meeting* » de l'IOWG organisé par le Comité permanent R à Bruxelles en avril 2024.

- Cette présence à Oslo a également été l'occasion de participer à la *European Intelligence Oversight Conference*. Cette conférence rassemblait des représentants d'institutions de contrôle des services de renseignement de seize pays ainsi que des participants d'organisations extérieures. Les thèmes de cette conférence étaient l'utilisation de données disponibles sur le marché, la planification des audits, la jurisprudence récente de la Cour européenne des droits de l'Homme, les bases techniques d'un contrôle efficace et les opportunités et défis en matière de reddition de compte et de communication.

- Le Comité permanent R a accueilli, fin septembre 2023, une délégation allemande de la commission parlementaire chargée du contrôle des services de renseignement du Land de Brandebourg. Lors de cette visite de deux jours, le Comité a présenté à la délégation allemande l'architecture institutionnelle et sécuritaire belge ainsi que les missions légales du Comité permanent R à travers une série de présentations, suivies de discussions et d'un partage d'expériences. Par ailleurs, la Présidente de la Chambre et de la Commission de suivi a reçu la délégation, le Comité et plusieurs de ses collaborateurs pour un échange de vues.

- Enfin, fin novembre 2023, une délégation du Comité permanent R a participé à Washington à l'annuel *International Intelligence Oversight Forum* (IIOF). L'IIOF se veut une plateforme internationale pour les organes de contrôle en matière de renseignement, de vie privée et de protection des données et pour d'autres parties prenantes, dont les services de renseignement et de sécurité, afin de discuter des développements (inter)nationaux et des *best practices*.

ANNEXES

Abréviations

ANS	Autorité nationale de sécurité
APD	Autorité de protection des données
BDC	Banques de données communes
BNG	Banque de données nationale générale
C.O.C.	Organe de contrôle de l'information policière
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
Convention 108	Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel
EMB	Exécutif des Musulmans de Belgique
IOWG	*Intelligence Oversight Working Group*
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.R&S	Loi du 30 novembre 1998 organique des services de renseignement et de sécurité
LFP	Loi du 5 août 1992 sur la fonction de police
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)
M.B.	Moniteur belge
MRD	Méthodes de recueil des données
OCAM	Organe de coordination pour l'analyse de la menace
SGRS	Service Général du Renseignement et de la Sécurité
Stratégie TER	Note stratégique Extrémisme et Terrorisme
UE	Union européenne
VSSE	Sûreté de l'État