Comité R | I
Contrôle des services de renseignement

RAPPORT D'ACTIVITÉS

2025

RAPPORT D'ACTIVITÉS

2025

Table des matières

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, le Comité R/I a réalisé ce rapport annuel 2025 pour rendre compte de ses activités.

Au fil de ce rapport, le Comité expose les principales actions qu'il a menées en 2025, qu'il s'agisse des enquêtes de contrôle, des avis formulés ou encore du travail réalisé par les membres et le greffe de l'Organe de recours. Une attention particulière est également portée aux mesures spécifiques et exceptionnelles de recueil de données mises en œuvre par les services de renseignement en 2025, ainsi qu'aux modalités de leur contrôle.

Bruxelles, 7 avril 2026

Frédéric Givron
Greffier

Vanessa Samain
Présidente

Séverine Merckx
Membre francophone

Filip Vanneste
Membre néerlandophone

PRÉFACE

L'unanimité est rare mais il est un point sur lequel tout le monde semble s'accorder : l'année écoulée aura été marquée par de profonds bouleversements tant géopolitiques que sociétaux. Rarement depuis la Seconde Guerre mondiale le monde n'aura connu un tel cumul de tensions : conflits armés, désinformation, recul démocratique,... Ces facteurs mettent évidemment à l'épreuve notre sécurité mais pas seulement. Ils mettent à mal nos institutions, notre cohésion sociale ainsi que la confiance des citoyens dans l'action publique.

L'exemple d'autres pays européens montre à quel point il est difficile de rétablir l'indépendance institutionnelle lorsque celle-ci a été durablement compromise. Si la Belgique n'en est pas là, elle n'échappe malheureusement pas à cette tendance de fragilisation de l'Etat de droit puisque selon un rapport de l'Union pour les libertés civiles en Europe, la Belgique a, avec six autres pays, le statut peu enviable de « *pays en déclin* »...[1]

En ces temps troublés, la crédibilité démocratique du travail des services de renseignement et de sécurité passe par la nécessité d'un organe de contrôle fort, capable d'affirmer et d'assumer son rôle d'organe de contrôle indépendant. Cette mission, nous la portons avec d'autant plus de détermination que la confiance démocratique ne se décrète pas. Elle se gagne pied à pied avec patience et abnégation au travers d'un travail rigoureux, exigeant et constant.

En 2025, le travail n'a pas manqué. Le Comité R/I a clôturé plusieurs enquêtes de contrôle mais, surtout, en a initié trois nouvelles d'initiative démontrant sa volonté d'avancer quelles que soient les circonstances.

L'analyse des chiffres lors du contrôle des méthodes particulières de renseignement (MPR) montre que la tendance de ces dernières années se confirme : le nombre de méthodes mises en œuvre par la Sûreté de l'Etat (VSSE) et le Service Général du Renseignement et de la Sécurité (SGRS) continue d'augmenter. Les trois méthodes exceptionnelles les plus utilisées par le SGRS restent identiques à celles relevées les années précédentes : le service de renseignement militaire recourt ainsi principalement aux écoutes téléphoniques, aux intrusions informatiques et aux observations dans des lieux non accessibles au public. Du côté de la VSSE, la prise de connaissance des données d'appel et des données de localisation représente la très grande majorité des méthodes spécifiques mises en œuvre. Un constant récurrent mérite d'être souligné : la méthode de l'infiltration (réelle ou virtuelle) reste peu voire pas utilisée par les deux services.

Deux singularités marquent par ailleurs l'année 2025. Au-delà de l'accomplissement de ses missions habituelles (enquêtes de contrôle, avis, contrôle des MPR,...) le Comité R/I a été confronté à une saisine inédite de contrôle approfondi de la légalité des MPR dans un dossier judiciaire à la demande de la Chambre des mises en accusations de Bruxelles. Pour la première fois de son histoire, le Comité a rendu un avis préjudiciel au début de l'année 2025. Aussi, le Comité a été saisi d'un premier signalement en tant que canal de signalement externe pour le traitement des signalements d'atteintes à l'intégrité au sein de la VSSE et du SGRS. Le Comité avait d'ores et déjà anticipé cette nouvelle compétence légale par la création d'une cellule spécifique.

1 Civil Liberties Union for Europe, *Liberties Rule of Law Report 2026*, www.liberties.eu.

Avant de conclure, impossible de ne pas évoquer la situation préoccupante de l'Organe de recours dont le Comité R/I assure la présidence et le greffe. En 2025, les recours ont littéralement explosé notamment en raison de l'élargissement des secteurs soumis à avis ou habilitation de sécurité. Soucieux de continuer à traiter les dossiers dans un délai raisonnable, le Comité R/I a réagi et augmenté significativement le nombre d'audiences. Néanmoins, au vu de l'ensemble des missions octroyées au Comité et malgré la bonne volonté des représentants d'instances tierces siégeant également à l'Organe de recours, l'augmentation du rythme atteint aujourd'hui ses limites. La poursuite de la digitalisation du greffe, amorcée en 2024, est demeurée une priorité. Grâce à l'investissement de l'ensemble du personnel du greffe de l'Organe de recours, nous espérons pouvoir mener ce projet à son terme au cours de l'année 2026.

Si la tendance se confirme, le risque de saturation est réel et posera un choix impossible à opérer entre le respect des délais raisonnables, la qualité des décisions et les impératifs de sécurité nationale. Surtout, cette évolution menace la mission principale et prioritaire du Comité : le contrôle des services de renseignement et de sécurité.

Enfin, le Comité n'a pas mis de côté les réformes nécessaires à son fonctionnement interne et a mené de front plusieurs projets.

Tout d'abord, il va de soi qu'assurer un travail de qualité à la hauteur des défis actuels passe par une politique de ressources humaines ambitieuse. Cette année, le cadre du Comité R/I s'est enrichi de nouveaux membres du personnel, venus renforcer pratiquement tous les départements. Grâce à ces renforts, le Comité peut travailler de manière moderne et professionnelle, notamment à travers l'élaboration d'un véritable plan d'audit à mettre en œuvre en 2026 et d'un plan stratégique pluriannuel.

Après 35 ans d'existence, il est ensuite apparu que l'identité visuelle du Comité nécessitait un « *rafraîchissement* ». Plus qu'une opération purement esthétique, nous souhaitions que ce nouveau logo soit l'expression visible des transformations profondes et des modernisations que nous entreprenons en interne. Fruit d'une réflexion collective de longue haleine, nous sommes particulièrement fiers du résultat qui reflète les principes de légalité, d'intégrité, d'indépendance et de transparence qui guident l'action du Comité.

Pour terminer, plus qu'un paragraphe convenu, je veux ici remercier sincèrement l'ensemble des membres du Comité pour leur engagement constant au service de l'intérêt général. Derrière les missions de plus en plus nombreuses et diverses du Comité, il y a des femmes et des hommes déterminés à contribuer à un État plus transparent, plus juste et plus sûr.

L'année 2026 s'annonce exigeante, mais je suis convaincue que grâce à la force de notre collectif, à la clarté de notre vision et à la solidité de nos valeurs, nous saurons relever les défis qui se présentent. Ensemble, en maintenant le cap, nous arriverons à bon port.

C'est une présidente enthousiaste et fière du travail de l'ensemble des membres du Comité R/I qui vous souhaite une bonne lecture de notre rapport d'activité 2025.

Vanessa Samain
7 avril 2026

ENQUÊTES DE CONTRÔLE

DES ÉCLAIRAGES THÉMATIQUES

1. ENQUÊTES CLÔTURÉES

1.1. Les menaces envers les opposants politiques présents en Belgique

En juin 2023, quelques semaines après la libération d'un humanitaire belge (et de trois autres Européens) détenu(s) arbitrairement en Iran pendant plus d'un an, l'octroi de visas à une délégation iranienne en visite à Bruxelles créait la controverse. Invités à participer au *Brussels Urban Summit*, réunion internationale des maires des grandes villes, quatorze représentants iraniens, dont le maire de Téhéran, se sont vus octroyer des visas « à territorialité limitée » par la Belgique. Les révélations quant aux activités présumées de surveillance et d'espionnage d'opposants iraniens par des membres de la délégation ont fait l'objet d'un vif débat dans la presse et au Parlement. Dans ce contexte, la Commission d'accompagnement des Comités P et R/I avait sollicité l'ouverture d'une enquête de contrôle commune relative à la position d'information de l'OCAM sur la menace que pouvait représenter la délégation iranienne. Cette enquête avait fait l'objet d'un premier rapport commun des Comités P et R/I démontrant l'implication réduite de l'OCAM dans ce dossier, limitée à une double évaluation de la menace à l'égard de l'événement et du maire de Téhéran.[1]

Au-delà de cet épisode précis, la Commission d'accompagnement sollicitait l'ouverture d'une seconde enquête de contrôle, plus large, sur l'évaluation par l'OCAM de la menace à l'égard d'opposants à des régimes autoritaires présents en Belgique. Dans cette enquête, les Comités ont choisi d'examiner plus particulièrement (1) le cadre légal et réglementaire dans lequel l'OCAM agit et les compétences dont il dispose (ou non) dans l'analyse des « régimes autoritaires » et de leurs activités en Belgique et (2) le cas échéant, de quelle manière l'OCAM procède à des analyses et évaluations des menaces potentielles à l'encontre d'opposants à ces régimes. Il s'agissait également d'interroger la pertinence des notions de « régimes autoritaires » et d'« opposants » ainsi que la façon dont l'OCAM les opérationnalise au quotidien.

L'analyse du cadre légal a confirmé que les éventuelles menaces, terroristes ou extrémistes, contre des « *opposants aux régimes autoritaires présents en Belgique* » font partie du champ de compétences de l'Organe de Coordination. L'OCAM peut donc réaliser des évaluations ponctuelles et/ou des analyses stratégiques sur cette thématique. En pratique toutefois, les notions de « régime autoritaire » et d' « opposant politique » se sont révélées être non pertinentes pour l'OCAM. En effet, celui-ci travaille à partir d'hypothèses quant à l'existence, réelle ou supposée, d'une menace terroriste et/ou extrémiste. Il n'y a pas de suivi systématique (et dès lors pas de définition ou d'opérationnalisation) de ces catégories, qui peuvent par contre apparaitre incidemment dans des évaluations. L'OCAM n'était pas en mesure de chiffrer les demandes d'évaluation qu'il reçoit concernant des éventuelles menaces liées (aux opposants) à un régime dit autoritaire. Selon l'Organe de Coordination, de telles demandes proviennent habituellement du Centre de Crise national et de la Direction centrale des opérations de police judiciaire de la Police fédérale.

1 COMITE R/I, *Rapport d'activités 2023*, p. 3 (« L'évaluation par l'OCAM de la menace sur une délégation iranienne à Bruxelles »). En parallèle, et toujours à la demande de la Commission de suivi, le Comité R/I a ouvert une enquête dédiée à la position d'information des services de renseignement (Comité R/I, *Enquête de contrôle sur la position d'information des services de renseignement et le suivi assuré à l'occasion de la visite d'une délégation iranienne à Bruxelles du 12 au 15 juin 2023 pour le Brussels Urban Summit, y compris la manière dont le processus de screening a été opéré en vue de la délivrance des visas aux membres de cette délégation*, www.comiteri.be).

À l'instar des évaluations ponctuelles de la menace, les analyses stratégiques sont toujours initiées à partir d'informations sur des menaces extrémistes et/ou terroristes (potentielles) en Belgique ou envers des intérêts belges à l'étranger. Depuis 2020, l'OCAM a par exemple dédié plusieurs analyses aux menaces terroristes et extrémistes liées au régime iranien à la suite de la tentative d'attentat contre un rassemblement d'opposants au régime de Téhéran à Villepinte (France) en 2018 et l'arrestation en Belgique dans ce cadre d'un couple belgo-iranien. De telles menaces sont décrites par l'OCAM comme relevant d'un « *contexte lié à l'étranger* », d'un « *contexte d'opposition politique à l'étranger ou de menace interétatique* ». Par ces termes, l'Organe de Coordination englobe « *l'ensemble des acteurs et des menaces liés aux conflits étrangers et/ou aux tensions politiques ayant un certain impact dans notre pays* ».[2] Les Comités P et R/I s'interrogeaient toutefois sur (la portée de) cette catégorie de menaces, dont l'intitulé varie d'un document à l'autre.

L'enquête a confirmé que les moyens de l'OCAM restent prioritairement dédiés au suivi des menaces en Belgique.

L'enquête des Comités P et R/I a également mis en lumière le flou qui demeure autour de la mission de l'OCAM vis-à-vis d'une « *menace étatique* ». En mars 2022, à la suite de l'invasion de l'Ukraine par la Russie, le Conseil national de sécurité chargeait l'OCAM d'examiner les menaces émanant de Russie, quelle que soit leur nature (« *all-threat assessment* »). Les Comités ont estimé qu'un tel mandat implique une potentielle extension des compétences de l'OCAM qui mérite d'être clarifiée et, le cas échéant, inscrite dans la loi.

Recommandations

› Définir les notions de « régime autoritaire » et d'« opposant » et clarifier la catégorie de « contexte lié à l'étranger »

Si aucun dysfonctionnement pouvant être lié au fait que l'OCAM n'a pas défini les notions de « régime autoritaire » ou d' « opposant » à ces régimes n'a pu être constaté au cours de l'enquête, les Comités P et R/I encouragent toutefois une concertation entre les partenaires belges – par exemple, dans le cadre de la Stratégie T.E.R. – afin de définir plus précisément, voire d'opérationnaliser, ces notions, ceci en vue d'une communication efficace entre les services. L'usage de différentes expressions concernant les menaces liées à un contexte étranger (« *contexte lié à l'étranger* », « *contexte d'opposition politique à l'étranger* », « *menace interétatique* ») et les confusions dans les réponses de l'OCAM sur les entités inscrites en BDC TER sèment le trouble quant à la portée de cette catégorie et aux compétences de l'Organe de Coordination en la matière. Les Comités P et R/I recommandent dès lors à l'OCAM de clarifier cette catégorie d'analyse.

2 OCAM, *Threat Trajectory 2023-2024*, réf. DOC OCAM/D/474035/139, p. 19.

› Travailler à des possibilités statistiques concernant les menaces liées à des « opposants »

L'OCAM n'était pas en mesure de fournir de statistiques sur les demandes d'évaluation qu'il reçoit concernant les menaces liées (aux opposants) à un régime dit autoritaire. Les Comités P et R/I encouragent l'OCAM à poursuivre ses efforts de traitement des informations entrantes et sortantes en vue de pouvoir produire des statistiques plus précises concernant, entre autres, les demandes d'évaluation qu'il reçoit.

1.2. Connaitre et contrôler le Cyber Command du SGRS[3]

À la mi-octobre 2022, le Ministère de la Défense a créé le Commandement cyber. Celui-ci a été intégré au sein du Service Général du Renseignement et de la Sécurité (SGRS) et, à ce titre, est soumis au contrôle du Comité R/I. Afin de garantir l'exercice efficace de ce contrôle, il était primordial pour le Comité de se familiariser pleinement avec ce nouveau commandement. En outre, l'objectif de faire évoluer le Commandement cyber vers une véritable Composante/Force cyber pourrait avoir des conséquences évidentes sur l'exercice des missions du Comité. Cette évolution soulève plusieurs questions fondamentales, notamment en ce qui concerne l'exercice des missions du SGRS dans le cyberespace et constituait, aux yeux du Comité, une raison supplémentaire d'ouvrir une enquête de contrôle dédiée Commandement cyber.

L'enquête a montré que les structures de contrôle internes et les instruments de gestion confirment, dans la pratique, l'intégration légale du Commandement cyber au sein du SGRS.

La capacité cyber du Commandement cyber assure actuellement l'exploitation du cyberespace au profit du SGRS et de la Défense et apporte, dans certains cas, son soutien à la Nation. En fonction de sa mission, la capacité cyber relève d'un cadre juridique différent : la Loi organique des services de renseignement et de sécurité (L.R&S) – dans ce cas, la responsabilité incombe au Commandement cyber du SGRS – ou bien l'Arrêté royal fixant la structure de la Défense et la Loi relative à la mise en œuvre et à la mise en condition de la Défense et son arrêté d'exécution, cas dans lequel la responsabilité incombe à la Force cyber. Bien que, d'un point de vue juridique, le Commandement cyber et la Force cyber soient deux entités distinctes au sein des forces de combat, ce n'est pas le cas sur le plan organisationnel. Le Commandant du Commandement cyber est également le Commandant de la Force cyber, et il existe une seule organisation au sein de laquelle tous les membres du personnel, le cas échéant, sont (doivent être) au service des deux entités. Alors que les missions et les compétences du Commandement cyber sont définies légalement dans la L.R&S, ce n'est pas le cas pour les missions de la Force cyber. D'autre part, les lignes hiérarchiques diffèrent selon que l'Unité cyber agit en tant qu'organe d'exécution du SGRS (Chef du SGRS)

3 Clôturée en décembre 2025, cette enquête a été présentée début 2026 à la Commission 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.

ou en tant que Force cyber (Chef de la Défense). Cette dualité dans la structure juridique, bien que compréhensible et justifiée, comporte un risque d'ambiguïté dans l'exécution des missions et l'exercice des compétences, et pourrait générer des discussions sur la compétence du Comité R/I en tant qu'organe de contrôle des activités de l'Unité cyber.

Recommandations

› Inscrire les missions spécifiques de la Force cyber dans l'Arrêté Royal du 30 juin 2025

Le Comité R/I recommande de décrire plus en détail, tout comme pour l'état-major renseignements et sécurité, les missions spécifiques de la Force cyber, donc de l'Unité cyber agissant comme force armée, dans l'A.R. du 30 juin 2025 fixant la structure générale du Ministère de la Défense et les attributions de certaines autorités. Le Comité recommande plus particulièrement au gouvernement de définir de manière concrète, par arrêté royal, les formes d'engagement opérationnel de la Force cyber et, le cas échéant, les formes d'aide et d'assistance militaires.

Le Comité rappelle que la Force cyber ne peut en aucun cas être chargée, au point de vue réglementaire ou opérationnel, de mener des activités de renseignement, telles que visées à l'article 11 L.R&S, ni de l'exécution des missions de sécurité décrites dans cette disposition et dans la Loi Classification. A cet égard, le Comité attire en outre l'attention sur le fait que les activités relevant du champ d'application légal du maintien de la sécurité militaire (art. 11 § 1er, 2° L.R&S) ou de la protection du secret militaire (art. 11, § 1er, 3°L.R&S) ne peuvent être confiées à la Force cyber.

› Conférer une valeur juridique à la réunion de commandement organisée au sein du SGRS

Au sein du SGRS, il est d'usage d'organiser une réunion de commandement toutes les deux semaines entre le Chef du SGRS, le chef adjoint, le Commissaire en chef et le Commissaire en chef adjoint, le Commandant cyber ainsi que les directeurs de toutes les directions. Cette réunion de commandement fait *de facto* office de comité de direction du SGRS. Le Comité R/I recommande de conférer une valeur juridique à cette réunion dans un arrêté royal ou ministériel.[4] Une telle réunion, organisée de manière réglementaire, permettrait de confirmer une bonne pratique et de la consolider juridiquement. De plus, cela créerait une obligation pour le Chef du SGRS et le Commandant cyber de se concerter formellement, et ce en vue d'une intégration plus poussée du Commandement cyber au sein du SGRS.

› Evaluer les services et produits fournis

Le Plan stratégique national de renseignement (PSNR) de 2022 prévoit une coopération renforcée dans le domaine cyber entre la VSSE et le SGRS. Ce plan indique que, compte tenu de l'augmentation des ressources prévues, le SGRS apporte un appui à ses partenaires nationaux, qui se traduit notamment par l'utilisation des capacités de collecte et d'analyse du SGRS en faveur de la VSSE.

Au cours de son enquête, le Comité a recueilli des éléments faisant apparaître que la VSSE aurait peu utilisé les capacités cyber du SGRS. Néanmoins, le Comité estime que le SGRS devrait procéder à

4 En comparaison, le comité de direction de la VSSE et sa composition ont été fixés par arrêté royal (art. 4 de l'A.R. du 5 décembre 2006 relatif à l'administration générale de la Sûreté de l'Etat).

une évaluation quantitative et qualitative des services et produits fournis par l'unité à d'autres organismes, et ce tant pour les clients de la Défense que pour les clients externes. Etant donné les attentes du gouvernement telles qu'énoncées dans le Plan stratégique national de renseignement, il convient de prêter une attention accrue aux services et aux produits fournis à la VSSE.

› Assurer un budget adéquat pour l'Unité cyber

La situation géopolitique actuelle exige une attention accrue pour la capacité cyber de la Défense belge. L'organisation administrative et juridique du Commandement cyber et de la Force cyber constitue une première étape. Le Comité recommande que le gouvernement et la Défense accordent une attention suffisante aux moyens nécessaires permettant de faire face aux nombreuses attentes des autorités politiques et militaires à l'égard de cette unité. Le Comité recommande à cet égard que le budget des Unités cyber comparables dans les Etats membres de l'OTAN soit pris comme référence.

› Maintenir la compétence « de contre-attaque » auprès du SGRS

Au cours de l'enquête de contrôle, le SGRS a annoncé avoir lancé une étude visant à déterminer si une modification de la L.R&S s'imposait en ce qui concerne les missions cyber spécifiques du SGRS et, en particulier, la compétence dite « de contre-attaque ».[5] Le SGRS et l'Unité cyber envisagent la suppression de cette compétence comme compétence du SGRS (Commandement cyber) et son transfert à la Force cyber. Le Comité estime toutefois qu'un tel transfert ne va pas de soi. Le pouvoir de mener une contre-attaque à la suite d'une cyberattaque est indissociable des missions de renseignement et de sécurité du SGRS. De plus, un tel transfert juridique à la Force cyber ne serait possible que si celle-ci était établie comme entité par la loi. Le Comité ne voit aucune raison pour que la Force cyber soit établie par une loi si les autres forces de combat, tel que prévu par la Constitution pour l'organisation des Forces armées, sont établies par arrêté royal.

Par ailleurs, le Comité rappelle que le gouvernement a récemment choisi de lier cette compétence au Commandement cyber (*cf.* le rapport au Roi joint à l'A.R. Structure de la Défense du 30 juin 2025).

› Prévoir l'affectation du personnel à la Force cyber

Le Comité constate que le gouvernement a décidé de créer la Force cyber comme force armée distincte. Dans le même temps, il convient de constater que si, pour diverses raisons, chaque membre du personnel militaire est affecté à une force déterminée, cela n'a pas été prévu lors de la création de la Force cyber. En application de cette réglementation, chaque militaire appartient aux Forces terrestre, aérienne, à la Marine, au Service médical ou au personnel civil. Le Comité recommande d'examiner dans quelle mesure une catégorie 'Force cyber' peut être ajoutée au fonctionnement des régimes mentionnés.

5 Cette mission s'inscrit à la fois dans le cadre de la mission de sécurité (à savoir neutraliser une cyberattaque) et dans celui de la mission renseignement (à savoir identifier les auteurs de la cyberattaque). Le législateur a jugé nécessaire de donner le droit au SGRS de contre-attaquer face à une cyberattaque aux fins de protection de la sécurité militaire (cette compétence a été attribuée via l'art. 4 Loi MRD du 4 février 2010).

› **Autoriser la Commission parlementaire de suivi des missions militaires à confier des enquêtes de contrôle au Comité R/I**

Le Comité est habilité à prendre l'initiative d'ouvrir une enquête de contrôle sur l'Unité cyber agissant en tant que Force cyber. Dans ce contexte, le Comité recommande que la Commission parlementaire de suivi des missions militaires, chargée du contrôle parlementaire des aspects opérationnels des Forces armées et, partant, des activités de la cybercapacité militaire dans le cadre d'une opération militaire, soit rendue légalement compétente pour confier au Comité R/I la réalisation d'enquêtes de contrôle sur la capacité cyber agissant en tant que Force cyber.[6] Au sein du Parlement fédéral, la Commission d'accompagnement et les commissions d'enquête parlementaires ont déjà le pouvoir de charger le Comité R/I de réaliser des enquêtes de contrôle.

1.3. Un rapport français (contesté) sur les Frères musulmans[7]

En 2021, le Comité R/I réalisait à la demande de la Commission d'accompagnement une enquête de contrôle relative au suivi par les services de renseignement des Frères musulmans et de la menace éventuelle que ceux-ci constituent en Belgique. La publication, en mai 2025, d'un rapport intitulé « *Frères musulmans et islamisme politique en France* »[8] a relancé le débat sur la menace que représente le mouvement. Très critique envers la Belgique, le rapport a suscité des débats à la Chambre, et la Commission de suivi a sollicité le Comité R/I en vue d'actualiser l'enquête de contrôle de 2021 et d'évaluer l'état d'avancement des recommandations qui y étaient formulées.[9]

Le Comité note tout d'abord que, depuis 2024, la VSSE et le SGRS assurent ensemble le suivi des Frères musulmans au sein de la plateforme commune *Counter Extremism & Counter Terrorism* (PFCECT). Le Comité y voit une réponse adéquate à sa recommandation d'un renforcement de la coopération entre les deux services dans cette matière. Le Comité salue également la définition commune du phénomène sur laquelle se sont accordés la VSSE, le SGRS et leurs partenaires de sécurité. Le phénomène fait en outre désormais l'objet d'un suivi structurel au sein de la Stratégie T.E.R., notamment dans le cadre du Groupe de Travail Extrémisme Islamique. Concernant la recommandation d'une plus grande sensibilisation des autorités, des administrations et du public vis-à-vis de la menace, le Comité relève les initiatives de la VSSE et, dans une moindre mesure, du SGRS, en vue d'améliorer la concertation avec les partenaires, via la diffusion de notes, l'organisation de briefings de sécurité et la tenue de réunions de coordination. La VSSE a par ailleurs profité de plusieurs de ses rapports annuels pour sensibiliser le grand public à la problématique des Frères musulmans. Le Comité ne disposait d'aucune information quant à l'état d'avancement de la recommandation relative à la vérification de l'intégrité, de la loyauté et de la discrétion comme préalable à l'exercice de certaines fonctions sensibles.

Quant à l'image de la menace, la PFCECT estime à une centaine le nombre d'individus participant activement à la diffusion de l'idéologie des Frères musulmans et identifie quelques dizaines d'organisations proches des Frères musulmans en Belgique. Parmi les évolutions constatées, la PFCECT pointe

6 Le Comité ne vise pas à exercer un contrôle sur les activités opérationnelles de la Force cyber mais entend éviter que des activités de renseignement menées au sein de la Force cyber échappent au contrôle.

7 Clôturée en décembre 2025, cette enquête a été présentée début 2026 à la Commission d'accompagnement.

8 Ministère de l'Intérieur, *Frères Musulmans et Islamisme Politique en France*, disponible sur le site www.interieur.fgouv.fr.

9 Comité R/I, *Rapport d'activités 2021*, pp. 61-67 (« Une attention renouvelée pour les Frères Musulmans »).

la réduction des financements de la Confrérie, l'apparition de nouvelles initiatives d'enseignement religieux en ligne et le repli de certains acteurs vers la Belgique suite aux pressions sécuritaires des autorités françaises.

À ce jour, selon les services de renseignement, les Frères musulmans ne posent pas directement de menace en termes d'actions violentes en Belgique ou envers des intérêts belges. Les services considèrent cependant toujours que leur idéologie encourage le développement d'un climat de polarisation. À ce titre, cette idéologie est considérée comme un possible vecteur de radicalisation pour certains profils. La menace représentée par les partisans de cette idéologie est donc à évaluer au cas par cas. La PFCECT s'attend à ce que la menace reste stable au cours des cinq prochaines années. Les Frères musulmans continueront probablement à diffuser leur idéologie, mais de manière limitée au vu de la diminution de leurs ressources financières.

La perception du phénomène par l'OCAM diffère de celle de la PFCECT et n'a pas varié depuis 2021 : il n'identifie aucune menace directe susceptible d'entraîner, à court ou long terme, une augmentation du niveau de la menace.

Concernant les conclusions du rapport français sur la présence des Frères Musulmans en Belgique, l'analyse de la PFCECT ne correspond pas entièrement à celle reprise dans le rapport français : la PFCECT ne voit pas d'indication qu'un contrôle serait exercé en Belgique par des islamistes et considère l'influence des Frères musulmans comme étant plus limitée que ce que suggère le rapport français.

2. ENQUÊTES DE CONTRÔLE EN COURS

2.1. La méthodologie d'analyse de la VSSE et du SGRS

Au quotidien, la VSSE et le SGRS procèdent à des analyses individuelles de la menace dans lesquelles ils attribuent des qualifications à des individus. Ces analyses peuvent, à différents stades d'une enquête de renseignement et pour diverses raisons, faire l'objet de communications externes vers des partenaires et des administrations. De telles communications sont susceptibles d'entrainer des conséquences négatives très concrètes sur les droits et libertés des citoyens puisqu'elles peuvent déboucher sur des décisions administratives qui les affectent de manière significative (par exemple, le refus ou le retrait d'une habilitation de sécurité, le refus de délivrance ou le retrait d'une autorisation de séjour, le refus d'octroi de la nationalité belge, le gel des avoirs, etc.). L'analyse des services de renseignement et les qualifications utilisées sont toutefois parfois contestées par les intéressés – notamment au moyen de plaintes introduites auprès du Comité.

Afin de faire la lumière sur les coulisses des analyses individuelles de la menace et sur la manière dont les résultats de ces analyses sont communiqués à des tiers, le Comité R/I a ouvert en 2023 une enquête de contrôle sur la méthodologie d'analyse utilisée par les services de renseignement et de sécurité pour la qualification de personnes.

L'enquête a été relancée en 2025 après une interruption de plusieurs mois due, entre autres, au traitement et à la finalisation de dossiers prioritaires du Comité. Des questions complémentaires ont été envoyées au SGRS et à la VSSE et le Comité R/I a rencontré les services pour clarifier certains aspects de leur méthodologie. Des vérifications ont en outre été effectuées sur l'intranet de la VSSE. A travers ces devoirs d'enquête, le Comité a notamment examiné les outils mis à disposition des collaborateurs du SGRS et de la VSSE pour les accompagner dans la rédaction d'analyses ainsi que les processus de contrôle qualité prévus en interne.[10]

2.2. La méthodologie d'analyse de l'OCAM

En parallèle de son enquête de contrôle dédiée à la méthodologie d'analyse de la VSSE et du SGRS, le Comité R/I a ouvert une enquête conjointe avec le Comité P afin d'examiner la méthodologie d'analyse de la menace mobilisée par l'OCAM.

Également suspendue au profit de dossiers jugés prioritaires, l'enquête a été relancée en 2025. Des questions complémentaires ont été posées à l'OCAM, qui y a apporté des réponses écrites et au cours d'un entretien. La documentation interne de l'OCAM, en particulier le manuel de son outil d'évaluation de la menace, a été soigneusement épluchée. Dans le cadre de cette enquête, les Comités P et R/I ont prêté une attention particulière aux indicateurs de risque mobilisés par l'OCAM dans son analyse de la menace, aux efforts déployés par l'Organe de coordination pour familiariser son personnel à cet outil ainsi qu'au contrôle qualité organisé en interne.[11]

2.3. Quelles (tentatives de) synergies entre les deux services de renseignement ?

Parmi les failles identifiées dans la chaine de sécurité belge par la Commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016, le manque de coopération entre les services de sécurité et « *l'absence d'une culture de partage de l'information* » étaient pointés du doigt. Dans ses recommandations, la Commission d'enquête a porté une attention particulière au renforcement de la coopération entre les deux services de renseignement. Le Comité R/I a également appelé, à de nombreuses reprises au cours de ses enquêtes de contrôle, à une meilleure coordination entre la VSSE et le SGRS.

En réponse à ces constats et recommandations, le SGRS et la VSSE ont élaboré en 2018 un Plan stratégique national du renseignement (PSNR). Validé par le Conseil national de sécurité, une version révisée a été publiée en 2022. L'objectif du PSNR est, à travers une coopération rapprochée, de soutenir les services dans l'accomplissement de leurs missions respectives, de renforcer leur position d'information et de rationaliser les ressources. Le document organise la coopération entre les deux services dans plusieurs domaines, par exemple en matière de contre-terrorisme, de contre-espionnage ou plus spécifiquement au niveau informatique et dans l'organisation des formations. Au PSNR,

10 Une version déclassifiée du rapport d'enquête a été présentée à la Commission d'accompagnement en 2026.

11 Une synthèse déclassifiée du rapport a été présentée à la Commission d'accompagnement en 2026.

s'ajoutent d'autres instruments ou protocoles d'accord qui prévoient un rapprochement, voire une coordination, entre la VSSE et le SGRS autour de projets spécifiques.

Dans ce contexte, le Comité a choisi d'ouvrir une enquête de contrôle afin d'identifier et d'évaluer les synergies existantes et planifiées entre les deux services de renseignement. Les synergies y sont définies comme des formes de coopération durable, entre la VSSE et le SGRS exclusivement, ayant pour caractéristique de mutualiser des ressources (par ex. humaines, financières, informationnelles ou matérielles) pour améliorer l'efficacité du point de vue des opérations ou des fonctions de support. L'enquête vise à examiner dans quelle mesure les synergies prévues dans les plans d'action et documents stratégiques sont effectivement mises en œuvre et avec quel degré d'efficacité.

2.4. Un opposant politique agressé à Tirlemont

Fin août 2025, le bourgmestre de Tirlemont adressait un courrier au Comité R/I à propos de l'agression d'un opposant politique congolais sur le territoire de sa commune. Très vite après les faits, les premières recherches en sources ouvertes indiquaient que ce dernier faisait l'objet d'un avis de recherche émis par les autorités congolaises. Le bourgmestre s'insurgeait de ne pas avoir été informé par les services de renseignement et de sécurité, en sa qualité d'autorité de police administrative, de l'existence d'une menace contre un résident de sa commune.

Ce dossier individuel fait écho à des défis connus et déjà examinés dans des enquêtes antérieures du Comité, en particulier sur les activités des services de renseignement étrangers vis-à-vis de leur diaspora en Belgique ou sur la communication de renseignements vers des instances tierces. Il apparaissait pertinent de se pencher sur un éventuel dysfonctionnement des services de renseignement et d'examiner la gestion de ce dossier par la VSSE et le SGRS au regard des recommandations formulées.

L'enquête du Comité R/I porte sur la position d'information des services quant à la menace visant l'intéressé, c'est-à-dire les informations collectées par la VSSE et le SGRS ainsi que les moyens et ressources déployés pour enrichir cette collecte. L'enquête s'intéresse également à l'échange d'informations, dans le cadre de ce dossier, entre les deux services de renseignement et vers d'autres partenaires.

3. AUTRES ACTIVITÉS DE CONTRÔLE

En avril 2025, le Comité a effectué une visite à l'étranger afin d'examiner la contribution belge à une opération multinationale de partage d'informations en matière de contre-terrorisme. Des visites de contrôle relatives à des opérations du SGRS ont été également été réalisées au mois d'avril 2025 au Moyen-Orient.

Pour des raisons de classification, les résultats de ces contrôles ne peuvent pas être partagés au moyen d'un rapportage externe.

MÉTHODES DE RENSEIGNEMENT, MESURES D'APPUI ET COLLECTE À L'ÉTRANGER

LA COLLECTE D'INFORMATIONS ET SES BALISES LÉGALES

Les sections qui suivent sont consacrées au contrôle des méthodes de renseignement auxquelles une attention particulière est accordée par le Comité qui agit, en ce qui concerne les méthodes particulières de renseignement, en tant qu'organe juridictionnel. Une section est également dédiée aux mesures d'appui auxquelles les services de renseignement peuvent recourir en appui de leurs opérations. Enfin, une dernière section a trait aux interceptions à l'étranger, prises d'images et intrusions dans des systèmes informatiques auxquelles le SGRS peut procéder.

1. LES MÉTHODES DE RENSEIGNEMENT

Avant de rendre compte du nombre de méthodes (particulières) de renseignement autorisées par les services de renseignement en 2025, ainsi que du contrôle effectué par le Comité sur ces méthodes, un bref rappel de ce qu'est une méthode de renseignement s'impose.

1.1. Qu'est-ce qu'une méthode de renseignement ?

Pour recueillir des données, les services de renseignement belges peuvent faire usage de trois catégories de méthodes de renseignement : les méthodes ordinaires, spécifiques et exceptionnelles. Introduite par le législateur en 2010, cette distinction vise à catégoriser les méthodes selon leur degré d'intrusion dans la vie privée, suivant l'idée que plus la méthode est intrusive, plus son utilisation doit être soumise à des procédures et à un contrôle stricts.

1.1.1. Les méthodes ordinaires

La catégorie de méthodes dites ordinaires regroupe les méthodes de recueil d'informations pour lesquels le législateur n'a, à l'origine, pas imposé de contrôle externe préalable particulier en raison d'une ingérence dans la vie privée jugée plus faible. Toutes les méthodes relevant de cette catégorie tombaient donc uniquement sous le champ du contrôle régulier du Comité R/I.

L'observation et l'inspection de lieux accessibles au public sans moyen technique (par exemple : suivre une personne en rue sans la filmer) ainsi que le recours à des sources humaines (informateurs) relèvent de cette catégorie.

Depuis 2016, de nouvelles méthodes ordinaires, dites méthodes ordinaires « plus », ont été introduites 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. L'obligation de contrôle ou d'information est réglée différemment pour chacune de ces méthodes.[12]

Appartiennent à cette catégorie notamment :
- La consultation d'images enregistrées par les caméras des services de police ;
- L'identification de l'abonné d'un service ou d'un moyen de télécommunication (par ex. un numéro de GSM ou une adresse IP) réalisée sans avoir recours à un moyen technique mais au moyen d'une réquisition auprès d'un opérateur/fournisseur ;
- L'identification des produits ou services financiers utilisés par une personne ou société déterminée ou vice-versa (par exemple, la vérification de l'identité liée à un numéro de compte bancaire connu).

1.1.2. Les méthodes spécifiques et exceptionnelles

Les services de renseignement peuvent également avoir recours aux méthodes particulières de renseignement (MPR). Celles-ci regroupent les méthodes spécifiques et les méthodes exceptionnelles de renseignement. Le recours à ce type de méthode doit se faire dans le respect des principes de légalité, de proportionnalité et de subsidiarité. Le service de renseignement devra démontrer que l'information qu'il recherche, en lien avec ses missions, ne pourrait pas raisonnablement être collectée au moyen d'une méthode moins intrusive (telle qu'une méthode ordinaire). L'ampleur des moyens déployés devront également être proportionnels au niveau de la menace évaluée par le service.

Les méthodes spécifiques recouvrent par exemple :
- La prise de connaissance des données d'appel et de localisation d'une communication électronique ;
- L'observation et l'inspection de lieux accessibles au public à l'aide de moyens techniques (par ex. la prise de photos ou de vidéos en rue lors d'une filature).

Les méthodes exceptionnelles recouvrent par exemple :
- L'intrusion dans un système informatique ;
- L'écoute, la prise de connaissance et l'enregistrement de communications privées ;
- L'obtention d'informations sur les transactions, comptes et actifs d'une personne ciblée, ainsi qu'un placement sous surveillance de ses transactions (monitoring en temps réel).

Au regard de leur caractère plus intrusif, les méthodes particulières de renseignement sont soumises à un **double contrôle externe** qui diffère selon que la méthode soit spécifique ou exceptionnelle.

12 Voy. Comité R/I, *Rapport d'activités 2022*, pp. 81-86.

La Commission administrative chargée du contrôle des méthodes spécifiques et exceptionnelles de recueil des données (Commission BIM) exerce un **contrôle *a priori*** de la légalité et du respect des principes de proportionnalité et de subsidiarité de chaque méthode particulière de renseignement. Elle doit être informée de toute décision de mise en œuvre d'une méthode spécifique et doit donner son accord explicite avant qu'un service puisse faire usage d'une méthode exceptionnelle.

Le Comité R/I est, quant à lui, chargé du **contrôle *a posteriori*** de ces méthodes. Il vérifie la légalité des décisions relatives aux méthodes spécifiques et exceptionnelles ainsi que le respect des principes de proportionnalité et de subsidiarité.

Le Comité agit en tant qu'organe juridictionnel. Son accord préalable n'est pas nécessaire pour la mise en œuvre d'une MPR mais lorsqu'il constate une illégalité ou le non-respect des principes de proportionnalité ou de subsidiarité, le Comité met fin à ladite méthode si celle-ci est encore en exécution. En tant qu'autorité de protection des données, il ordonne par ailleurs l'interdiction d'exploitation et la destruction des informations récoltées.

1.1.3. Illustration : de l'observation ordinaire à l'observation exceptionnelle

Dans l'exemple fictif ci-dessous, le service de renseignement procède d'abord à une méthode ordinaire, avant d'avoir recours à une méthode spécifique puis exceptionnelle pour collecter les informations recherchées. Ce cas met en lumière les principes de légalité, de proportionnalité et de subsidiarité ainsi que le renforcement des mécanismes de contrôle et de traçabilité pour les méthodes plus intrusives.

Un individu est signalé pour des contacts répétés avec un milieu extrémiste susceptible de présenter une menace pour la sécurité nationale. A ce stade, aucun élément concret ne permet d'établir l'existence d'un projet précis. Le service met en œuvre une **méthode ordinaire d'observation (art. 16/1 L.R&S)** : surveillance discrète dans des lieux accessibles au public, suivi des déplacements, identification des fréquentations. L'observation se limite à ce qui est visible dans l'espace public, sans recours à des moyens techniques intrusifs. Concrètement, il s'agira d'une filature au cours de laquelle l'individu sera suivi par un ou plusieurs membres du service et observé à distance. Le service peut effectuer cette méthode sans devoir informer ni la Commission BIM ni le Comité R/I.

Les observations révèlent des rencontres régulières potentiellement problématiques dans un bâtiment déterminé et des allées et venues inhabituelles, notamment à des horaires nocturnes. Le service souhaite mieux objectiver ces éléments. Si la menace potentielle est suffisamment caractérisée et que les méthodes ordinaires de recueil de données

sont jugées insuffisantes, le service recourt à **une méthode spécifique d'observation (art. 18/4 L.R&S)**. Concrètement, il peut s'agir de l'installation d'une caméra dans la rue, orientée vers l'entrée du bâtiment, afin de documenter de manière structurée les allées et venues. L'observation demeure extérieure et porte exclusivement sur ce qui est perceptible depuis la voie publique, mais elle repose désormais sur un moyen technique permettant un enregistrement continu. Cette méthode spécifique doit être notifiée à la Commission BIM avant qu'elle ne puisse être exécutée. La Commission en informe le Comité R/I. Les deux organes de contrôle peuvent à tout moment mettre fin à l'exécution de la méthode s'ils estiment que les conditions de légalité, de proportionnalité ou de subsidiarité ne sont plus rencontrées.

Enfin, les éléments recueillis laissent supposer que des préparatifs concrets pourraient être en cours à l'intérieur du bâtiment et qu'une action violente est envisagée. Les méthodes précédentes ne permettent pas d'établir la nature exacte des activités menées à l'abri des regards, et d'autres méthodes spécifiques ne le permettraient pas non plus. Une **méthode exceptionnelle d'observation (art. 18/11 L.R&S)** peut alors être autorisée, par exemple l'installation discrète d'une caméra à l'intérieur du lieu non accessible au public afin d'observer ce qui s'y déroule. Cette mesure implique une ingérence particulièrement élevée dans la vie privée et n'est mise en œuvre qu'en présence d'une menace potentielle grave pour la sécurité nationale et suivant un cadre juridique strict. Avant que cette méthode puisse être mise en œuvre, l'autorisation de la Commission BIM est nécessaire. Le Comité effectue ensuite également un contrôle *a posteriori* de la méthode.

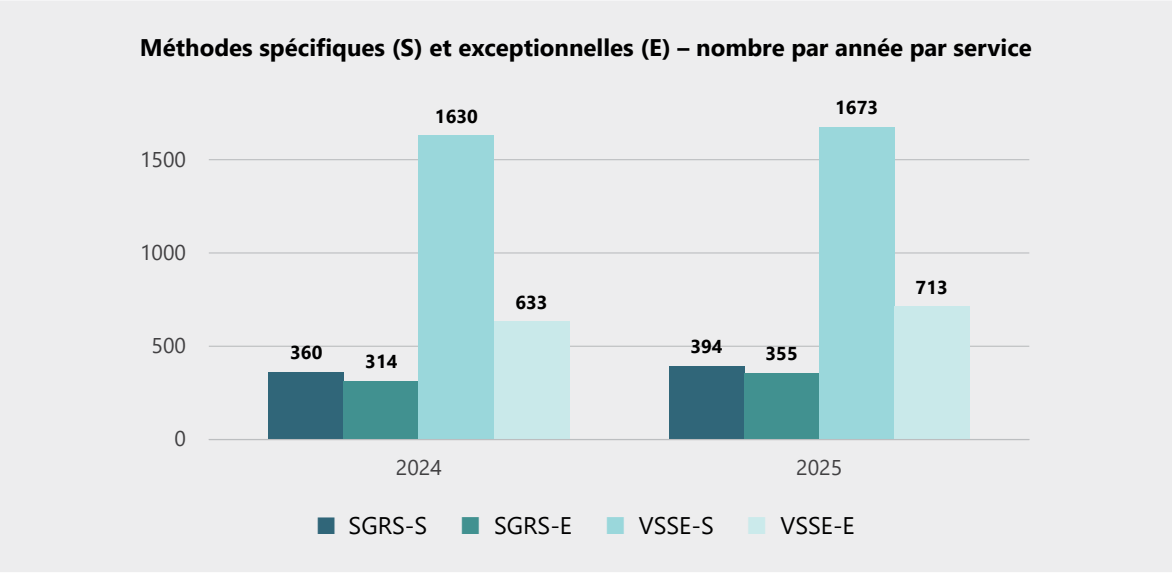
1.2. Les chiffres relatifs aux méthodes particulières et à certaines méthodes ordinaires

1.2.1. Tendances générales

Entre le 1er janvier et le 31 décembre 2025, **3 135 méthodes particulières de renseignement** ont été autorisées par les deux services de renseignement confondus : 749 méthodes déployées par le SGRS et 2 386 méthodes déployées par la VSSE. Ceci correspond à une **croissance de 6,7% en comparaison à l'année 2024** (où 2937 méthodes particulières avaient été comptabilisées).[13]

13 Afin de disposer d'un aperçu quantitatif global, le Comité compatibilise le nombre effectif de méthodes déployées par les services. Il est important de noter que les services de renseignement s'appuient sur une autre méthode pour la comptabilisation. Il est question de dossiers MPR (également appelés dossiers BIM), un dossier consistant généralement en le déploiement de plusieurs méthodes (2,25 méthodes par dossier en 2025, contre 2,19 pour 2024). Cela s'explique notamment par le fait que certaines méthodes ne peuvent être dissociées d'autres. Par exemple, la mise en œuvre d'une écoute téléphonique, qui est une méthode exceptionnelle (art. 18/17 L.R&S), ne peut se faire sans la prise de connaissance des métadonnées d'appel, qui est une méthode spécifique (art. 18/8, §1er, 1° L.R&S). Entre le 1er janvier et le 31 décembre 2025, 1389 dossiers MPR (également appelés dossiers BIM) ont été établis par les deux services de renseignement confondus pour l'utilisation des méthodes particulières de renseignement :1152 dossiers MPR par la VSSE (735 dossiers relatifs à des méthodes spécifiques et 417 à des méthodes exceptionnelles) et 237 dossiers MPR pour le SGRS (112 dossiers relatifs à des méthodes spécifiques et 125 à des méthodes exceptionnelles).

Le graphique ci-après rend compte de l'évolution du nombre de méthodes spécifiques et exceptionnelles par service de 2024 à 2025.



On observe une réalité quelque peu différente pour les deux services. Le nombre de MPR mises en œuvre par la VSSE est considérablement plus élevé que celui du SGRS. Ce constat est posé depuis de nombreuses années. En 2024 et en 2025, la proportion des MPR de la VSSE représentait chaque fois plus des trois quarts de l'ensemble.

Dans la mesure où le SGRS exerce une partie importante de ses compétences dans un contexte orienté vers l'étranger et que, sur le territoire national, ses missions se concentrent principalement sur des enjeux liés au domaine militaire, il est logique que le nombre de MPR qu'il mette en œuvre soit inférieur à celui de la VSSE, dont les compétences sont principalement exercées dans un cadre intérieur plus large. A l'étranger, le SGRS peut également faire usage de l'art. 44 L.R&S en ce qui concerne les interceptions, prises d'images et intrusions dans des systèmes informatiques.[14]

Le nombre de méthodes spécifiques et exceptionnelles mises en œuvre par le service de renseignement militaire connaît toutefois une progression de 2024 à 2025, d'environ 10%, pour les deux types de méthodes. Le SGRS déploie plus de méthodes spécifiques qu'exceptionnelles, mais dans une proportion nettement moindre que la VSSE. Ce constat est valide pour 2024 et 2025.

En ce qui concerne la VSSE, la courbe de progression afférente au nombre de méthodes spécifiques déployées en 2024 et 2025 est en légère augmentation (+ 3%) tandis que celle des méthodes exceptionnelles est plus marquée (+ 13%). Comme évoqué *supra*, le nombre de méthodes spécifiques reste nettement plus élevé en 2025 que celui des méthodes exceptionnelles : les méthodes spécifiques représentent ainsi systématiquement plus de 70% des MPR déployées par la VSSE. Le constat avait déjà été posé en 2024 et confirme la tendance, observée depuis plusieurs années déjà, d'une augmentation des MPR déployées.

14 Voy. à ce propos « *3. Interceptions à l'étranger, prises d'images et intrusions dans des systèmes informatiques* ».

1.2.2. Les méthodes déployées par le SGRS

Entre le 1er janvier et le 31 décembre 2025, **749 méthodes particulières de renseignement ont été déployées par le SGRS**, dont 394 spécifiques et 355 exceptionnelles.[15]

Les tableaux, graphiques et explicatifs ci-après détaillent les méthodes déployées par le SGRS au cours de l'année 2025, et offrent une analyse condensée de leur évolution par rapport à l'année précédente.

Les méthodes spécifiques (SGRS)

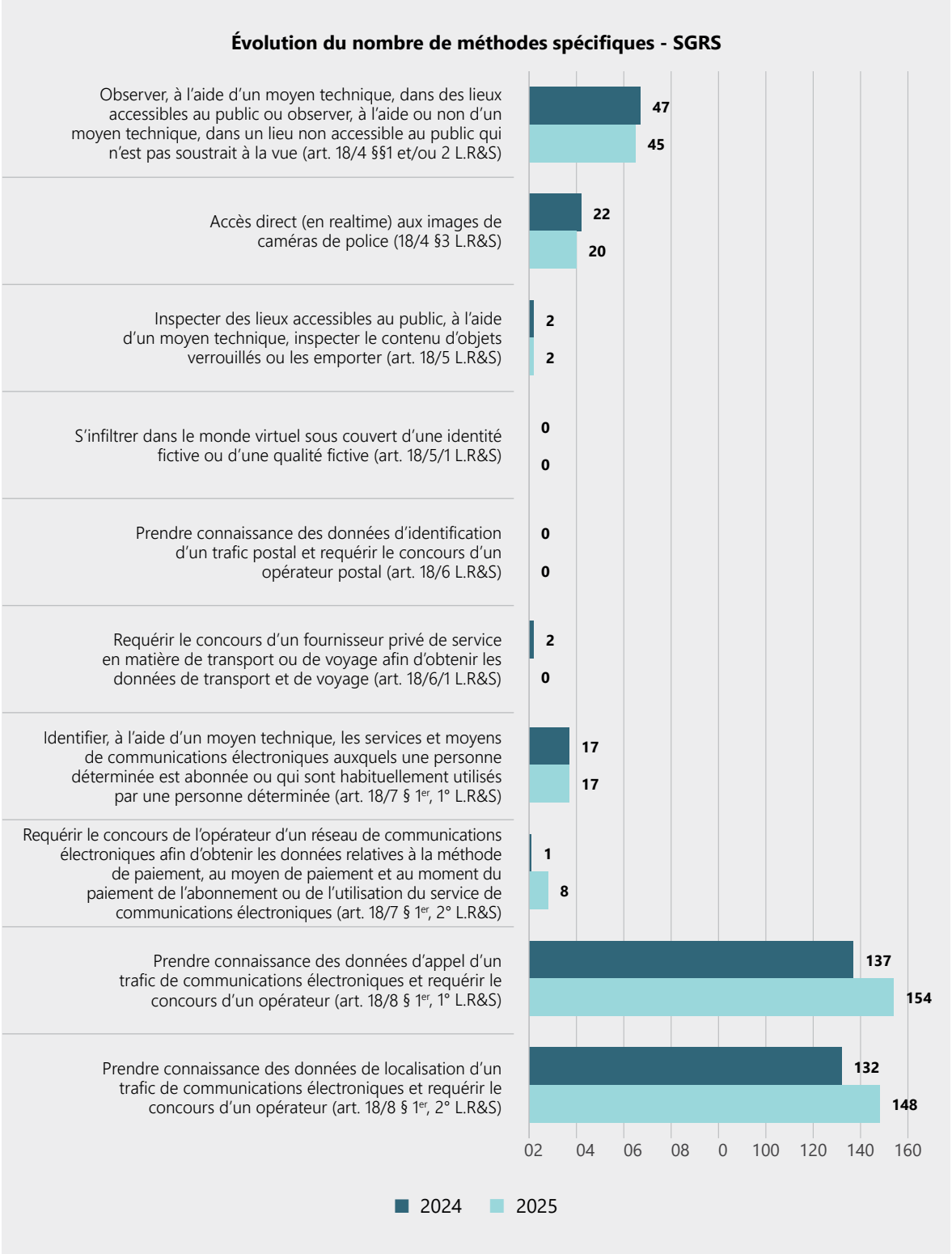
Méthodes spécifiques (SGRS)	2025
Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 §§1 et/ou 2 L.R&S)	45
Accès direct (en *realtime*) aux images de caméras de police (18/4 §3 L.R&S)	20
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)	2
S'infiltrer dans le monde virtuel sous couvert d'une identité fictive ou d'une qualité fictive (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)	17
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)	8
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)	154
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)	148
TOTAL	**394**

La prise de connaissance des données d'appel d'un trafic de communications électroniques ainsi que des données de localisation (art. 18/8, §1er, 1° et 2° L.R&S) demeurent les deux méthodes spécifiques les plus utilisées par le SGRS. Ces méthodes sont généralement déployées ensemble, ce qui explique que leur nombre est presque identique. L'observation à l'aide d'un moyen technique ou dans un lieu non accessible au public (art. 18/4 §§1 et/ou 2 L.R&S) reste la troisième méthode la plus utilisée par le service militaire.

Si l'on compare ces chiffres avec ceux de 2024, on constate que le nombre de méthodes spécifiques mises en œuvre par le service de renseignement militaire augmente de 2024 à 2025, de 9%.

15 Pour 237 dossiers MPR, avec une moyenne de 3,2 méthodes par dossier.

Le graphique ci-après illustre l'évolution du recours aux méthodes spécifiques par le SGRS de 2024 à 2025. A y regarder de plus près, les tendances divergent. Il ressort en effet de cette comparaison que, bien que le nombre total de méthodes spécifiques soit en augmentation, le recours à certaines méthodes a légèrement diminué. C'est notamment le cas des observations ainsi que des accès directs aux images des caméras de police. Au contraire, les deux méthodes spécifiques les plus mobilisées (prise de connaissance des données de repérage et de localisation d'un trafic de communications électroniques (art. 18/8, §1er, 1° et 2° L.R&S)) enregistrent les plus grandes progressions.



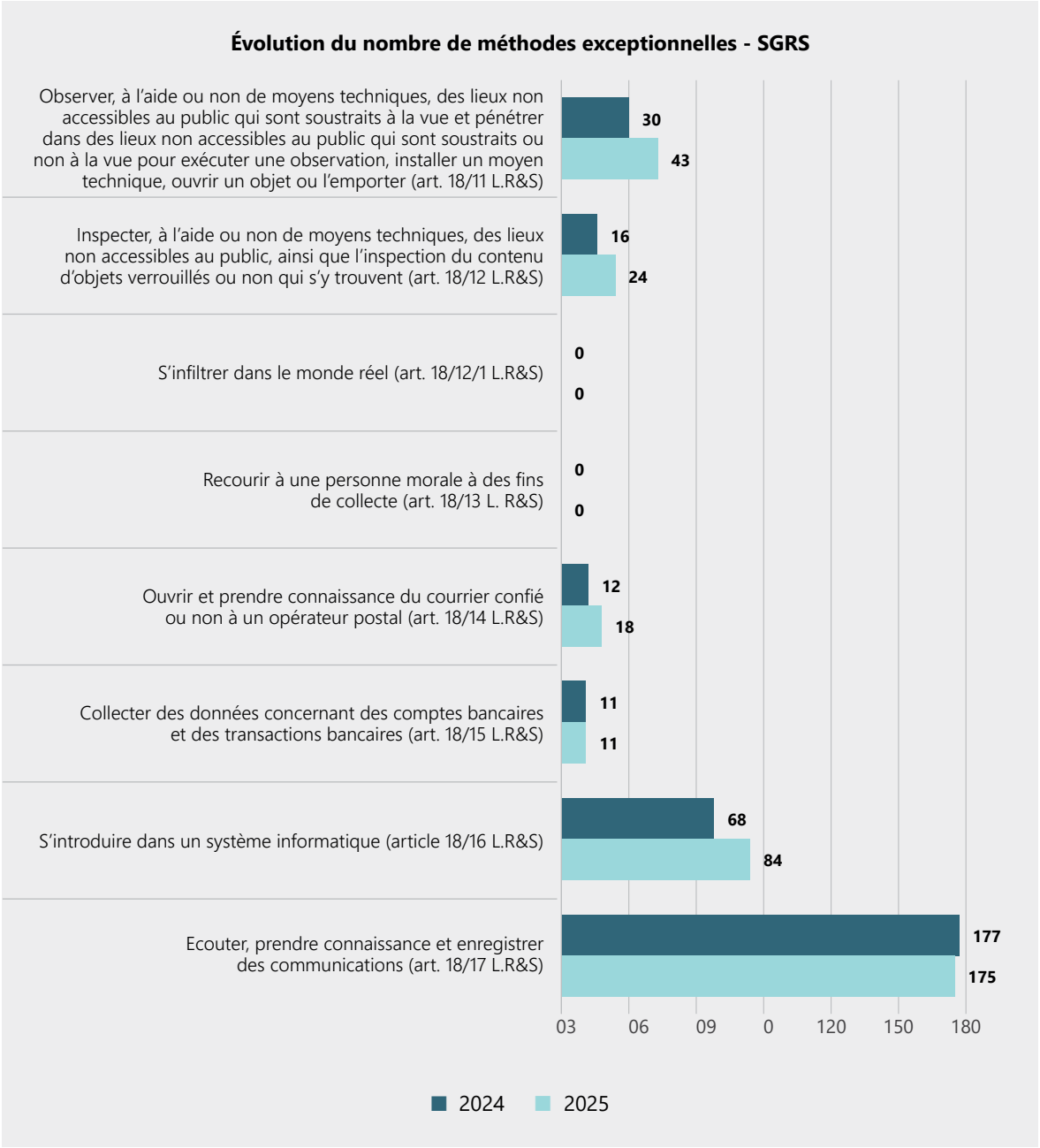
Les méthodes exceptionnelles (SGRS)

Méthodes exceptionnelles (SGRS)	2025
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)	43
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)	24
S'infiltrer dans le monde réel (art. 18/12/1 L.R&S)	0
Recourir à une personne morale à des fins de collecte (art. 18/13 L. R&S)	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	18
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	11
S'introduire dans un système informatique (art. 18/16 L.R&S)	84
Ecouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	175
TOTAL	**355**

Les écoutes téléphoniques (art. 18/17 L.R&S) ont été la méthode exceptionnelle privilégiée par le service militaire en 2025, constituant à elle seule près de la moitié du nombre total de méthodes exceptionnelles déployées au cours de l'année par le service. L'intrusion informatique (art. 18/16 L.R&S) et l'observation dans des lieux non accessibles au public (art. 18/11 L.R&S) se situent respectivement en deuxième et troisième positions. Ces constats s'inscrivent dans la tendance générale observée ces dernières années puisque ces méthodes constituaient déjà les trois méthodes exceptionnelles les plus utilisées par le service militaire en 2022, 2023 et 2024.

Le graphique ci-après illustre une nouvelle fois l'évolution du recours aux méthodes exceptionnelles par le SGRS de 2024 à 2025. Une comparaison avec les chiffres de 2024 indique que les méthodes exceptionnelles effectivement déployées par le SGRS en 2025 sont, par rapport à l'année précédente, globalement en augmentation. Par type de méthode, la tendance oscille entre augmentation et stagnation. Un très léger recul est observé pour les écoutes téléphoniques (art. 18/17 L.R&S). Les intrusions informatiques (art. 18/16 L.R&S) représentent au contraire la plus forte progression en chiffres nets en 2025 par rapport à 2024 au sein des méthodes exceptionnelles.

En 2024 et en 2025, le SGRS n'a pas fait usage de l'infiltration dans le monde réel, pas plus que de l'infiltration dans le monde virtuel (cette dernière est une méthode spécifique – voir le tableau dédié). En outre, il n'a pas eu recours à une personne morale à des fins de collecte. Ces observations valent également pour la VSSE.



Les menaces au titre desquelles des mesures spécifiques et exceptionnelles sont déployées (SGRS)

A l'instar de l'année précédente, l'espionnage est resté la menace pour laquelle le plus de MPR ont été déployées en 2025 par le SGRS.[16] Les MPR s'inscrivant dans le cadre de la lutte contre l'ingérence sont en augmentation. Les MPR en lien avec le crime organisé, bien que moins nombreuses, sont en nette augmentation. Le nombre de MPR qui concernent l'extrémisme et le terrorisme reste peu élevé. Ce qui n'est pas forcément une surprise, étant donné que, dans ces matières, le SGRS se focalise sur la situation à l'étranger et peut faire usage de l'article 44 L.R&S.[17]

16 Une méthode peut concerner plusieurs menaces.

17 Voy. à ce propos « *3. Interceptions à l'étranger, prises d'images et intrusions dans des systèmes informatiques* ».

Les méthodes ordinaires 'plus' (SGRS)

La L.R&S 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').[18] 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.

La comparaison avec les chiffres de 2024 témoigne d'une augmentation du recours à ces méthodes en 2025.

Méthodes ordinaires 'plus' (SGRS)	2025	2025
Identification de « l'abonné ou de l'utilisateur habituel » de télécommunications (art. 16/2 L.R&S)	**432**	**571**
Recherches ciblées de données PNR (art. 16/3/1 L.R&S)	**7**	**21**
Utilisation d'images de caméras de police (pas en *realtime*) (art. 16/4, §2 L.R&S)	**18**	**22**
Réquisition de certaines données financières (art. 16/6 L.R&S)	**23**	**27**

Ont augmenté d'environ 25% le recours à l'identification de « l'abonné ou de l'utilisateur habituel » de télécommunications (art. 16/2 L.R&S), l'utilisation d'images de caméras de police (pas en *realtime*) (art. 16/4, §2 L.R&S) et la réquisition de certaines données financières (art. 16/6 L.R&S).

L'utilisation de la méthode recherches ciblées de données PNR (art. 16/3/1 L.R&S) a quant à elle triplé en 2025. L'augmentation nette des chiffres liés à cette dernière méthode s'explique en réalité par le fait qu'une chute du nombre de recherches ciblées de données PNR avait été enregistrée en 2024, à la suite d'un arrêt de la Cour constitutionnelle du 12 octobre 2023 annulant l'article 16/3 L.R&S.[19] Cet arrêt empêchait la VSSE et le SGRS d'interroger la banque de données PNR. Une loi de réparation, prise par le législateur et entrée en vigueur le 15 juillet 2024, a permis aux services de renseignement d'interroger à nouveau la banque de données PNR, ce qui explique la reprise de ce type de méthodes mi-2024.

1.2.3. Les méthodes déployées par la VSSE

Entre le 1er janvier et le 31 décembre 2025, **2 386 méthodes particulières de renseignement ont été déployées par la VSSE**, dont 1 673 spécifiques et 713 exceptionnelles.[20]

18 Voy. à ce propos « *1.1. Qu'est-ce qu'une méthode de renseignement ?* ».

19 Dans son arrêt (arrêt 131/2023), la Cour constitutionnelle 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 constituait 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. Jusqu'à l'entrée en vigueur de la loi de réparation, les services de renseignement ne pouvaient plus interroger la banque de données PNR.

20 Pour 1152 dossiers MPR, avec une moyenne de deux méthodes par dossier.

Les tableaux, graphiques et explicatifs ci-après détaillent les méthodes déployées par la VSSE au cours de l'année 2025, et offrent une analyse condensée de leur évolution par rapport à l'année précédente.

Les méthodes spécifiques (VSSE)

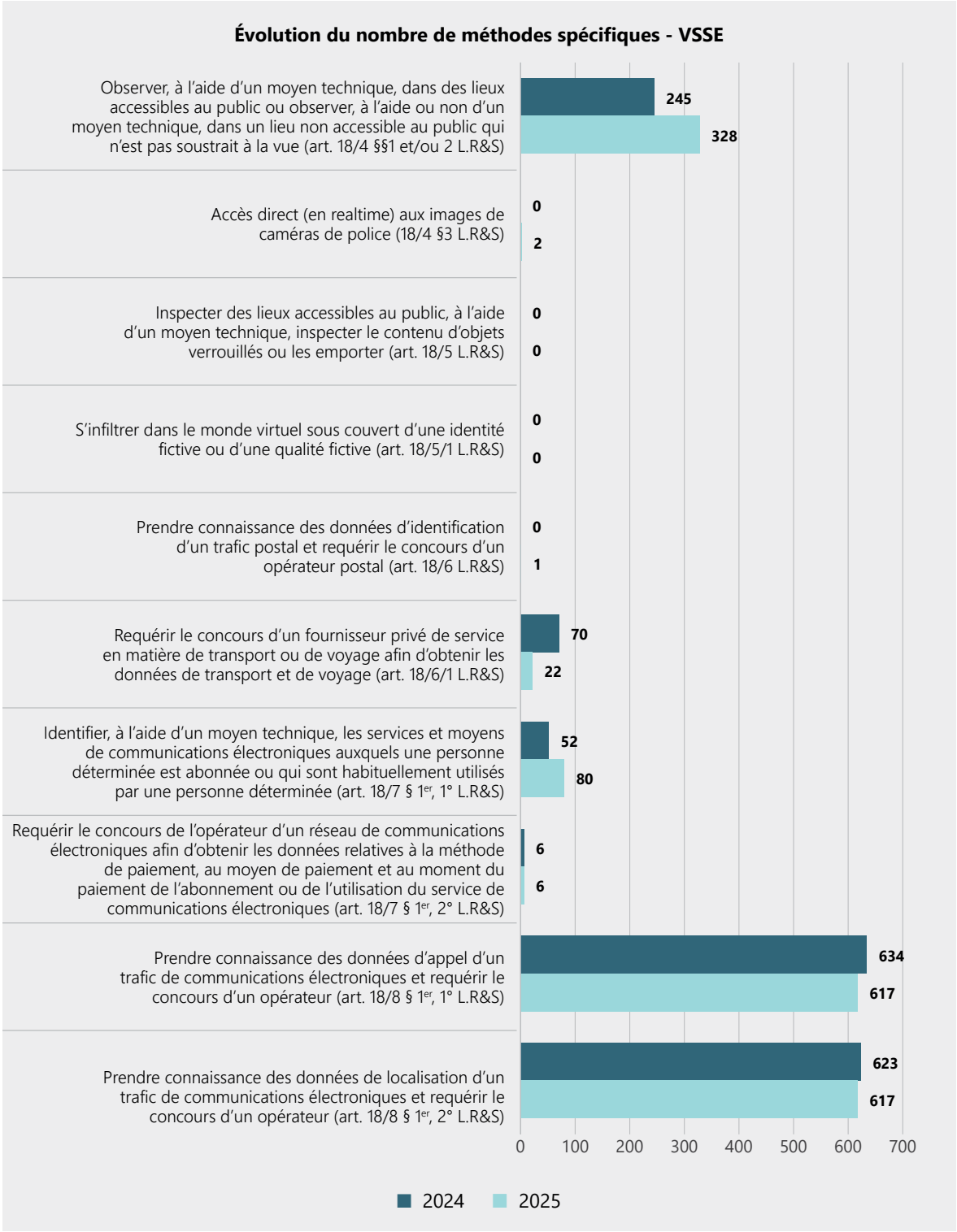
Méthodes spécifiques (VSSE)	2025
Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 §§1 et/ou 2 L.R&S)	328
Accès direct (en *realtime*) aux images de caméras de police (18/4 §3 L.R&S)	2
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'une identité fictive ou d'une qualité fictive (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)	1
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)	22
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)	80
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)	6
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)	617
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)	617
TOTAL	**1673**

En ce qui concerne les méthodes spécifiques les plus déployées en 2025, la prise de connaissance des données d'appel d'un trafic de communications électroniques ainsi que des données de localisation (art. 18/8, §1er, 1° et 2° L.R&S) sont les deux méthodes spécifiques les plus utilisées par le VSSE. A elles deux, elles représentent un peu moins des trois quarts des méthodes spécifiques déployées par la VSSE en 2025. Ces méthodes sont généralement déployées ensemble, ce qui explique que leur nombre est identique. L'observation à l'aide d'un moyen technique dans les lieux accessibles au public (art. 18/4 §§1 et/ou 2 L.R&S) constitue la troisième méthode la plus utilisée par le service civil. Ces trois méthodes sont également celles qui ont été le plus mobilisées par le SGRS parmi l'ensemble des mesures spécifiques (*cf.* ci-dessus).

Si l'on compare ces chiffres avec ceux de 2024, on constate que le nombre de méthodes spécifiques mises en œuvre par la VSSE n'augmente que marginalement de 2024 à 2025 (+ 43 unités, soit moins de 3 % d'augmentation). Leur répartition par méthode suit une tendance plutôt inégale. Ainsi, en ce qui concerne les deux méthodes spécifiques les plus mobilisées, leur nombre est en léger recul par rapport à 2024. On relève par contre une augmentation du nombre d'observations avec un moyen

technique ou dans un lieu non accessible au public (art. 18/4 §§1 et/ou 2 L.R&S) qui ont connu un bond de 33% en un an. Le recours au concours d'un fournisseur privé de transport ou de voyage art. 18/7 § 1er, 2° L.R&S) a quant à lui nettement diminué.

Enfin, il convient de noter que la VSSE n'a ni en 2024 ni en 2025 (pas plus qu'auparavant) fait usage de l'art. 18/5 L.R&S, qui prévoit la possibilité en cas de menace potentielle ressortant de la compétence du service, d'inspecter des lieux accessibles au public, à l'aide d'un moyen technique, et d'inspecter le contenu d'objets verrouillés qui s'y trouvent ou les emporter. Le service n'a pas non plus fait usage de l'infiltration dans le monde virtuel (art. 18/5/1 L.R&S). Cette observation vaut également pour le SGRS.



Les méthodes exceptionnelles (VSSE)

Méthodes exceptionnelles (VSSE)	2025
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)	22
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)	18
S'infiltrer dans le monde réel (art. 18/12/1 L.R&S)	0
Recourir à une personne morale à des fins de collecte (art. 18/13 L. R&S)	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	17
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	82
S'introduire dans un système informatique (art. 18/16 L.R&S)	101
Ecouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	473
TOTAL	**713**

La méthode la plus utilisée est l'écoute téléphonique (art. 18/17 L.R&S). Elle représente à elle seule plus de la moitié du nombre total de méthodes exceptionnelles auquel le service a eu recours en 2025. Une tendance similaire est observée concernant le SGRS (*cf.* ci-dessus). Vient ensuite l'intrusion dans un système informatique (art. 18/16 L.R&S) qui constitue également la deuxième méthode la plus mobilisée par le service de renseignement militaire. Mais à l'inverse, alors que la collecte de données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S) est une méthode qui a été peu mobilisée par le SGRS – une dizaine par an – et de manière stable, il s'agit de la troisième méthode la plus mobilisée par la VSSE en 2025.

Relevons enfin que la VSSE fait moins usage que le SGRS des méthodes d'observation et d'inspection de lieux non accessibles au public (artt. 18/11 et 18/12 L.R&S). La méthode exceptionnelle d'observation a été déployée 22 fois par la VSSE tandis que le SGRS la déployait à 43 reprises. La méthode exceptionnelle d'inspection a été mise en œuvre à 18 reprises par la VSSE en 2025, tandis que le SGRS y a eu recours 24 fois.

Une comparaison avec le nombre de méthodes exceptionnelles déployées par la VSSE en 2024 révèle que leur nombre a augmenté de 13 % entre 2024 et 2025 (augmentation nette de 80 unités). Le graphique ci-après illustre l'évolution du recours à chaque méthode exceptionnelle. Il nous apprend que deux des trois méthodes exceptionnelles les plus mobilisées par le service en 2025 sont en nette progression par rapport à l'année précédente. Il s'agit de l'écoute téléphonique (art. 18/17 L.R&S) ainsi que la collecte de données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S). Ces deux méthodes connaissent une nette progression de 2024 à 2025 (passant respectivement de 380 à 473 et de 59 à 82 unités). Cette tendance n'est pas observée auprès du SGRS, chez qui le nombre de recours à ces deux méthodes est resté stable (*cfr* ci-dessus). Enfin, alors que les intrusions informatiques (art. 18/16 L.R&S) représentent la plus forte progression en chiffres nets en 2025 par rapport à 2024 au sein des méthodes exceptionnelles pour le SGRS, le recours à cette méthode au sein de la VSSE est en léger recul par rapport à 2024.

De 2023 à 2025 inclus, la VSSE n'a pas fait usage de l'infiltration dans le monde réel, pas plus que de l'infiltration dans le monde virtuel (cette dernière est une méthode spécifique). En outre, elle n'a pas eu recours à une personne morale à des fins de collecte. Ces observations ont également été formulées pour le SGRS.

FOCUS : faux noms et identités fictives, fausses qualités et qualités fictives

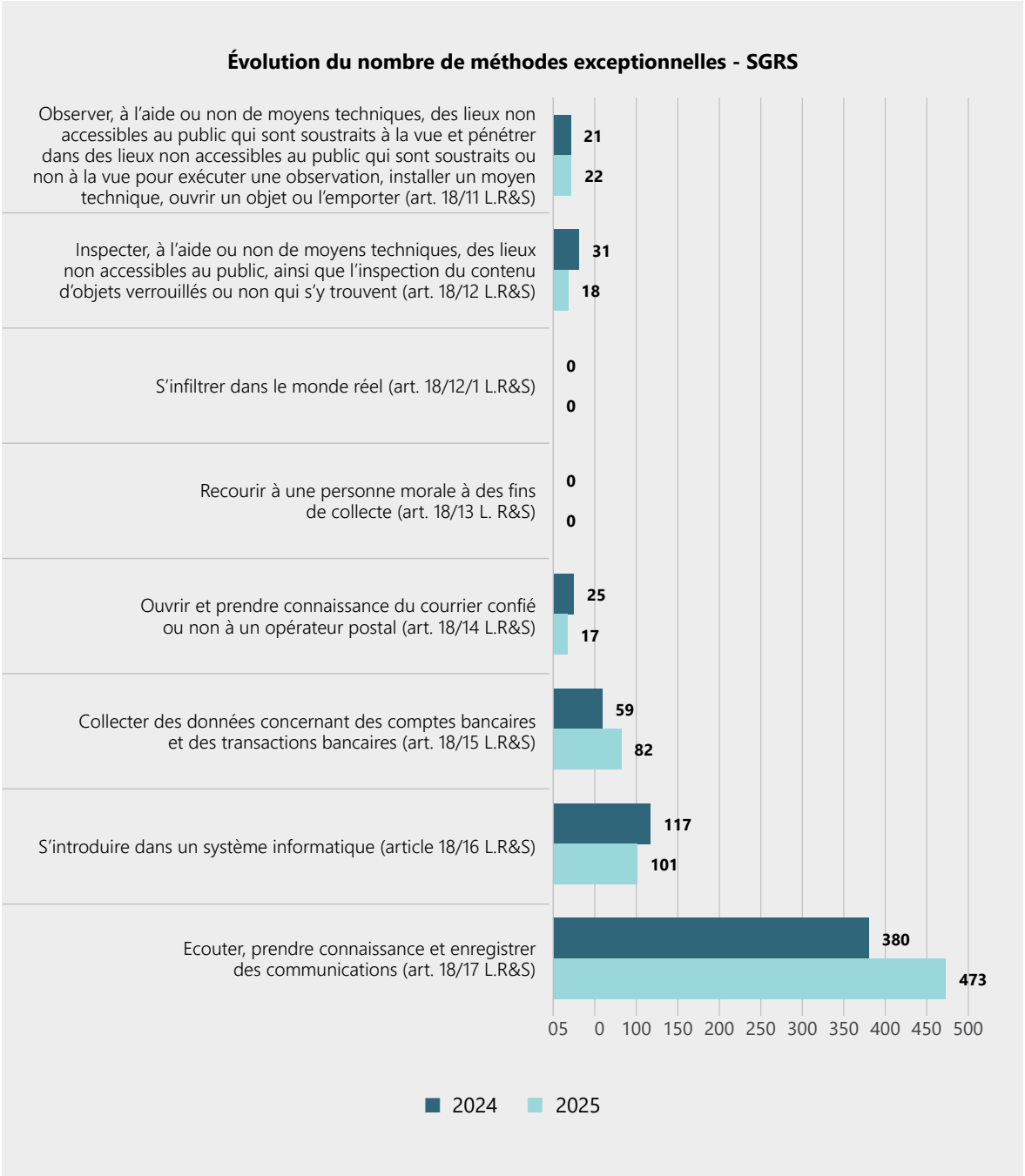
La L.R&S fait la distinction entre les faux noms et les identités fictives. Dans les deux cas, il s'agit pour un membre des services de renseignement et de sécurité d'utiliser un nom qui n'est pas le sien.

La principale différence concerne la preuve de ce nom : le **faux nom** n'est pas soutenu par la création de papiers d'identité officiels, alors que l'**identité fictive** est attestée par une carte d'identité, un passeport, une carte d'étranger ou un document de séjour. Le faux nom peut aussi être soutenu par des documents créés par le service de renseignement, tant qu'il ne s'agit pas des documents officiels listés pour l'identité fictive (ex : cartes de visites, CV, etc.).

La seconde différence est que le faux nom se limite à ce qu'il est, c'est-à-dire un nom et prénom d'emprunt alors que l'identité fictive est un concept plus large, pouvant recouvrir toutes les informations contenues dans les documents qui la soutiennent (un numéro de registre national, une date de naissance, une nationalité, etc.).

Les différences entre le faux nom et l'identité fictive correspondent donc à une gradation à la fois dans les informations couvertes, dans la crédibilité des informations d'emprunt et dans les ressources étatiques employées pour soutenir cette crédibilité.

La L.R&S va aussi permettre à un membre d'un service de renseignement de se prévaloir de qualités qui ne sont pas les siennes, par exemple une profession (ex : diplomate, professeur, électricien, etc..), un statut (ex : propriétaire, réfugié politique), un titre, ou une fonction. Une gradation existe ici aussi : s'il découle des effets juridiques de la qualité dont le membre des services se prévaut, il s'agit d'une **qualité fictive**. S'il ne découle aucun effet juridique particulier de la qualité dont l'agent se prévaut, il s'agira d'une **fausse qualité**.



Les menaces au titre desquelles des mesures spécifiques et exceptionnelles sont déployées (VSSE)

Comme en 2024, parmi les menaces suivies par le service de renseignement civil, le terrorisme et l'espionnage sont majoritaires en ce qui concerne le déploiement de MPR. A leur suite, en termes de nombres de MPR déployées, on retrouve les menaces d'ingérence et d'extrémisme. A une moindre échelle, la VSSE met en œuvre de plus en plus de méthodes dans le cadre de la lutte contre la criminalité organisée.

Les méthodes ordinaires 'plus' (VSSE)

A l'exception de l'utilisation d'images de caméras de police (pas en *realtime*) qui est en baisse, le recours à ces méthodes par la VSSE a connu une augmentation considérable en 2025. L'identification de « l'abonné ou de l'utilisateur habituel » de télécommunications (c'est-à-dire de l'identité de la personne liée à la carte SIM) passant de 5 543 à 6 439, les réquisitions de certaines données financières de 229 à 330 et les recherches ciblées de données PNR de 74 en 2024 à 207 en 2025. L'augmentation drastique des chiffres liés à cette dernière méthode, également constaté pour le SGRS, s'explique en réalité par le fait qu'une chute du nombre de recherches ciblées de données PNR avait été enregistrée en 2024, à la suite d'un arrêt de la Cour constitutionnelle du 12 octobre 2023 annulant l'article 16/3 L.R&S.[21]

Méthodes ordinaires 'plus' (VSSE)	2025	2025
Identification de « l'abonné ou de l'utilisateur habituel » de télécommunications (art. 16/2 L.R&S)	**5543**	**6439**
Recherches ciblées de données PNR (art. 16/3/1 L.R&S)	**74**	**207**
Utilisation d'images de caméras de police (pas en *realtime*) (art. 16/4, §2 L.R&S)	**76**	**53**
Réquisition de certaines données financières (art. 16/6 L.R&S)	**229**	**330**

1.3. Le contrôle exercé par le Comité R/I

Cette section porte sur le contrôle exercé par le Comité R/I sur les méthodes particulières de renseignement (MPR). Avant de parler du nombre ainsi que de la nature des décisions prises par le Comité R/I en 2025, la nature du contrôle exercé sur les MPR est précisé. Il sera également question de l'attention spécifique réservée par le Comité à certains profils lors du contrôle opéré sur les MPR ainsi que du premier avis préjudiciel rendu par le Comité en janvier 2025.

1.3.1. La nature du contrôle

Le contrôle exercé par le Comité est de nature juridictionnelle et porte sur la légalité, la proportionnalité et la subsidiarité des méthodes spécifiques et exceptionnelles de renseignement.

Le Comité ne doit pas marquer son accord avant la mise en œuvre d'une MPR mais il peut ordonner l'arrêt d'une méthode, l'interdiction d'exploitation des données collectées par une méthode et la destruction de ces données s'il constate des illégalités ou le non-respect du principe de proportionnalité ou de subsidiarité.

Afin d'assurer ce contrôle *a posteriori*, le Comité prend connaissance de l'ensemble des autorisations de mise en œuvre de MPR (art. 43/3 L.R&S). Si lors de l'**enquête *prima facie*** qu'il réalise, il suspecte des irrégularités, il se saisit du dossier pour effectuer un contrôle approfondi (art. 43/2 L.R&S).

21 Voy. ci-dessus.

Hormis cette saisine d'initiative, le Comité peut être saisi de quatre autres manières (art. 43/4 L.R&S) :

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

Une fois saisi, le Comité peut prendre plusieurs types de décisions[22] :

1. Mettre fin à la méthode concernée si celle-ci est toujours en cours ou si elle a été suspendue par la Commission BIM, et interdire l'exploitation des données recueillies grâce à cette méthode et leur destruction (art. 43/6 § 1er, alinéa 1er, L.R&S) ;
2. Mettre fin partiellement à une méthode autorisée ;
3. Lever totalement ou partiellement la suspension et l'interdiction qui ont été décidées par la Commission BIM (art. 43/6 § 1er, alinéa 1er, L.R&S). Ceci implique que la méthode autorisée par le dirigeant du service soit (partiellement) considérée comme légale, proportionnelle et subsidiaire par le Comité ;
4. Constater l'incompétence du Comité R/I ;
5. Déclarer le caractère infondé de l'affaire pendante et permettre la poursuite de la méthode.

Par ailleurs, le Comité peut aussi être saisi en sa qualité d'auteur d'avis préjudiciel (art. 131*bis*, 189*quater* et 279*bis* du Code d'instruction criminelle (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.

1.3.2. Le nombre de saisines en baisse

Pour l'année 2025, le Comité a été saisi à **douze reprises**. En nette baisse par rapport à l'année 2024 (23 saisines), ce nombre est comparable à l'année 2023 (13 saisines).

L'ensemble des saisines sont le résultat d'une suspension ordonnée par la Commission BIM. Cela signifie que lors du contrôle *prima facie* de l'ensemble des autorisations de mises en œuvre des méthodes particulières, le Comité n'a pas identifié d'éléments requérant une saisine d'initiative.

22 Sont seules visées ici les décisions finales. Plusieurs décisions intermédiaires peuvent intervenir dans le cadre du traitement d'un dossier (telles que l'audition des membres de la Commission BIM, la demande d'informations complémentaires du service de renseignement).

Type de saisine	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
1. D'initiative	16	3	1	1	4	2	1	5	0	0	0
2. Autorité de protection des données	0	0	0	0	0	0	0	0	0	0	0
3. Plainte	0	1	0	0	0	0	0	0	0	2	0
4. Interdiction d'exploitation par la Commission BIM	11	19	15	10	12	9	8	9	13	20	12
5. Autorisation du ministre	0	0	0	0	0	0	0	0	0	0	0
6. Auteur d'avis préjudiciel	0	0	0	0	0	0	0	0	0	1	0
TOTAL	**27**	**23**	**16**	**11**	**16**	**11**	**9**	**14**	**13**	**23**	**12**

Parmi ces douze saisines, quatre concernent le SGRS et huit la VSSE. Plusieurs autorisations concernaient des méthodes visant la/les même(s) personne(s) d'intérêt.

1.3.3. Des interdictions d'exploitation des données illégalement collectées et leur destruction ordonnée

Pour l'ensemble des saisines intervenues en 2025, il a été ordonné de mettre fin à la méthode et de détruire les données collectées illégalement.

Les décisions intervenues peuvent être réparties en quatre catégories, selon le type de problème constaté :

Accès à davantage de données que celles visées par la méthode

Trois interdictions d'exploitation sont le résultat d'erreurs ayant eu pour conséquence la mise à disposition de données excessives sur la personne ciblée. Dans deux cas, l'erreur est imputable au service tiers réquisitionné par le service de renseignement :

- Un service de renseignement souhaitait prendre connaissance, via une méthode exceptionnelle, des applications que deux cibles utilisaient et le contenu des échanges réalisés via ces applications (*datatap*). Trois numéros de téléphone étaient visés dans la demande. Après avoir reçu un avis conforme de la Commission BIM, la méthode a été exécutée par l'intermédiaire d'un service externe belge. Néanmoins, le service de renseignement a constaté avoir reçu des conversations téléphoniques classiques sur ces trois numéros de téléphone. Pourtant, elles n'avaient pas été réquisitionnées puisque selon les choix opérationnels du service concerné, seuls les échanges *data* étaient visés par la demande. S'apercevant de cette erreur, le chef de service en a informé la Commission BIM. Cette dernière a été contrainte de prononcer une interdiction d'exploitation de ces informations et a saisi le Comité. Celui-ci a déclaré que l'enregistrement des communications téléphoniques régulières était illégal. Il a ordonné que ces informations, illégalement obtenues, ne soient pas exploitées et soient détruites.
- Un cas similaire s'est produit quelques mois plus tard. Il concernait le même service de renseignement souhaitant réaliser une opération similaire (*datatap*) sur un numéro de téléphone mobile.

› Un service de renseignement souhaitait, par une méthode exceptionnelle, prendre connaissance d'informations relatives à certaines transactions bancaires effectuées sur un compte bancaire au cours d'une période définie de plusieurs mois. Seules certaines transactions bancaires étaient visées, à savoir celles faisant, dans leur communication, référence à un élément précis. Après avoir reçu un avis conforme de la Commission BIM, le service a fait appel à un opérateur pour l'exécution de la méthode. Par erreur, la réquisition envoyée à cet opérateur ne mentionnait pas le tri des transactions sur base de la communication. Bien que le service de renseignement ait rectifié cette erreur par l'envoi d'une nouvelle réquisition, le service avait reçu l'ensemble des transactions ayant été effectuées sur ce compte bancaire lors de la période ciblée. Informée par le chef du service de renseignement, la Commission BIM a constaté l'illégalité de ce recueil de données et en a interdit l'exploitation. Saisi par la Commission BIM, le Comité R/I a confirmé l'illégalité, a interdit l'exploitation de ces données et a ordonné leur destruction.

La collecte d'informations concernant une personne non ciblée

Trois autres décisions d'interdiction d'exploitation et de destruction des données illégales tiennent au fait que les données collectées concernaient des personnes qui n'étaient pas ciblées par le service de renseignement :

› Un service de renseignement souhaitait prendre connaissance, via des méthodes spécifique et exceptionnelle, des données d'appel et de localisation et du contenu des communications relatives à un numéro de téléphone d'une cible sur une période de temps déterminée. Plusieurs mois après l'exécution de ces méthodes, le service de renseignement a constaté que le numéro de téléphone sur lequel les méthodes avaient été exécutées concernait, non pas la cible, mais une autre personne portant le même prénom et nom de famille et évoluant dans le même milieu que la cible, ayant avec celle-ci de nombreuses connaissances communes. Le chef du service en a informé la Commission BIM qui a conclu que les informations collectées par la méthode étaient illégales et qu'elles ne pouvaient être exploitées. Le Comité R/I a confirmé le caractère illégal des données, l'interdiction d'exploitation de celles-ci et a ordonné leur destruction.

› Un service de renseignement avait lancé une méthode spécifique pour obtenir les données d'appel et de localisation d'un numéro de téléphone mobile. Pour l'exécution de la méthode, le concours d'un opérateur téléphonique avait été requis. Après le début de l'exécution de la méthode, le service s'est rendu compte qu'une erreur avait été commise dans le chef de l'opérateur qui avait transmis au service les données demandées d'un numéro de téléphone erroné. Le service de renseignement a signalé auprès de la Commission BIM cette erreur. Cette dernière a déclaré les informations collectées d'illégales, a interdit leur exploitation et a saisi le Comité R/I. Ce dernier a confirmé le caractère illégal des informations collectées, l'interdiction de leur exploitation et a ordonné leur destruction.

La collecte d'informations en dehors d'une période autorisée

Cinq décisions sont intervenues suite à des données collectées sur la personne ciblée en dehors de la période autorisée :

- Un service de renseignement entendait continuer d'observer, notamment avec des moyens techniques, les agissements d'une cible. Après avoir, au moyen d'une méthode spécifique, observé la cible, le service a, à plusieurs reprises, motivé une prolongation de cette observation. Ces méthodes spécifiques successives ne permettaient cependant pas au service d'observer la cible avec des moyens techniques pendant une période continue ; les périodes d'observation étant entrecoupées de quelques jours non couverts par une autorisation. Pourtant, pendant trois courtes périodes non autorisées, des données ont été collectées par le service via des moyens techniques. Plusieurs mois après l'exécution de cette observation, le service a averti la Commission BIM de cet incident. Celle-ci a constaté l'illégalité des données collectées pendant ces périodes et a prononcé l'interdiction de leur exploitation. Le Comité R/I a pris trois décisions confirmant cette lecture et ordonnant la destruction de ces données.
- Dans le cadre d'un autre dossier impliquant l'usage du même type de matériel d'observation, une erreur similaire s'est produite et a été rapportée, là encore, par le service à la Commission BIM. Après la décision d'interdiction d'exploitation prise par la Commission BIM, le Comité R/I a, lui aussi, déclaré les données collectées en dehors de la période autorisée comme étant illégales, a interdit leur exploitation et a ordonné leur destruction.
- Un service de renseignement avait lancé une méthode spécifique pour obtenir les données d'appel et de localisation d'un numéro de téléphone mobile pour une période limitée dans le temps. Néanmoins, l'opérateur a transmis au service de renseignement des données pour une période plus longue que celle figurant dans l'autorisation. Informée par le service de renseignement concerné, la Commission BIM a pris une décision d'interdiction d'exploitation des données collectées en dehors de la période couverte par l'autorisation. Saisi à son tour par la Commission BIM, le Comité R/I a confirmé le caractère illégal de ces données, interdit leur exploitation et ordonné leur destruction.

Non-respect du principe de proportionnalité

- Un service de renseignement souhaitait prolonger une méthode d'observation sur un véhicule. Cependant, sur la base des renseignements précédemment collectés par le service, il était apparu que le véhicule n'était plus utilisé par la personne ciblée. Par conséquent, la Commission BIM a conclu que la décision du dirigeant du service ne permettait pas de justifier la nécessité de la méthode spécifique estimant que les circonstances de fait ainsi que la motivation en matière de subsidiarité et de proportionnalité n'étaient pas suffisantes. Cette dernière a ordonné la suspension de la méthode concernée et interdit l'exploitation des données collectées. Saisi à son tour, le Comité R/I a confirmé le caractère illégal de la mesure, interdit l'exploitation des données collectées via celle-ci et ordonné la destruction de ces données.

1.3.4. Attention spécifique du Comité à l'égard de certains profils

Les professions protégées

La L.R&S prévoit que, lorsqu'une MPR vise un avocat, un médecin ou un journaliste, elle ne peut être autorisée que si elle est strictement nécessaire à l'accomplissement des missions légales des services et qu'aucune mesure moins intrusive n'est possible. L'autorisation est soumise à une procédure renforcée et à un contrôle spécifique. En outre, les informations couvertes par le secret professionnel ou la protection des sources ne peuvent être exploitées que dans la mesure strictement pertinente pour la menace concernée, afin de limiter l'atteinte aux droits fondamentaux.

En 2025, des MPR n'ont été déployées à l'encontre de professions bénéficiant d'une protection particulière que dans un nombre très limité de cas. Dans le cadre de sa mission de contrôle, le Comité a procédé aux vérifications nécessaires et a constaté que les garanties et conditions prévues par la loi étaient respectées.

Autres qualités : mandataires politiques et diplomates

La L.R&S ne prévoit, ni pour les mandataires politiques ni pour les diplomates, de régime de protection spécifique comparable à celui instauré pour les avocats, médecins ou journalistes. Toutefois, compte tenu de la nature particulière de leurs fonctions et de leur rôle institutionnel, il est nécessaire d'accorder une attention particulière à leur éventuelle implication lorsque des MPR sont mises en œuvre, afin d'en apprécier avec prudence la portée et les implications.

En 2025, des MPR n'ont été déployées à l'encontre de mandataires politiques et de diplomates que dans un faible nombre de cas. Le Comité a effectué sa mission de contrôle classique et a constaté que les garanties et conditions prévues par la loi étaient respectées.

1.3.5. Un premier avis préjudiciel rendu en janvier 2025

En 2024, le Comité R/I a été saisi, pour la première fois de son histoire, d'une demande d'avis préjudiciel sur la légalité de méthodes spécifiques et exceptionnelles, dont les données recueillies ont été utilisées dans le cadre d'une affaire pénale.[23] L'avis du Comité a été rendu en janvier 2025. Le déroulement de l'instruction ainsi qu'une réflexion sur un certain nombre de questions intervenues lors du contrôle sont résumés ci-dessous.

23 Indépendamment des différentes manières dont le Comité peut être saisi pour contrôler *a posteriori* des méthodes spécifiques et exceptionnelles de renseignement (voy. à ce propos le point « *1.3.1 La nature du contrôle* »), le Comité peut aussi être saisi en sa qualité d'« auteur d'avis préjudiciel » (articles 131*bis*, 189*quater* et 279*bis* du CIC). Le cas échéant, le Comité rend un avis sur la légalité des méthodes spécifiques ou exceptionnelles dont les données recueillies sont utilisées dans le cadre d'une affaire pénale. Les demandes d'avis sont introduites par les juridictions d'instruction ou par les juridictions de fond.

L'instruction du dossier et l'avis du Comité

La demande a été formulée devant la Chambre des mises en accusations de la Cour d'appel de Bruxelles par un inculpé qui souhaitait un contrôle anticipé de la régularité de la procédure initiée à son encontre.

Considérant qu'une lecture combinée des articles 235*bis* et 131*bis* du Code d'instruction criminelle (CIC) rend possible une demande d'avis du Comité lors du contrôle de la régularité de la procédure, et ce avant même le stade du règlement de la procédure, la Chambre des mises en accusation, par un arrêt du 24 septembre 2024, a demandé au Comité de se prononcer sur les méthodes spécifiques et exceptionnelles exécutées par la VSSE.

Dans cette affaire, la VSSE avait mis en œuvre un nombre significatif de méthodes spécifiques de recueil de données avant de rapporter à la Commission BIM l'existence de faits punissables, qui ont alors fait l'objet d'un procès-verbal déclassifié sur la base de l'article 19/1 de la L.R&S.

Après instruction du dossier, le Comité a conclu que les méthodes particulières de renseignement visées avaient été décidées et exécutées conformément à la loi.[24]

Ce dossier a également permis au Comité de se prononcer sur un certain nombre de questions, résumées ci-dessous, relatives à la portée de sa saisine ainsi que sur la concurrence entre une enquête pénale et une enquête de renseignement.

Portée de la saisine du Comité

A l'occasion de l'instruction, le Comité a constaté que la portée de sa saisine diffère selon qu'il est saisi d'un contrôle *a posteriori* sur la base des articles 43/2 et suivants de la L.R&S (par exemple à l'occasion d'une plainte) ou d'un avis préjudiciel sur la base du Code d'instruction criminelle (CIC).

En cas de plainte, conformément à l'article 43/2 de la L.R&S, le contrôle du Comité R/I porte sur la légalité, la proportionnalité et la subsidiarité des méthodes spécifiques et exceptionnelles de recueil de données, mises en œuvre par les services de renseignement et de sécurité à l'égard d'une personne justifiant d'un intérêt personnel. Dans ce cas, le Comité examine les méthodes particulières mises en œuvre par les deux services ayant spécifiquement ciblé la personne concernée ou, sans que celle-ci ne soit visée par les méthodes, ayant permis le recueil direct de données à caractère personnel la concernant. Par recueil direct, il faut entendre toute situation dans laquelle la personne concernée est elle-même l'origine des données recueillies à son sujet au cours de la mise en œuvre de la méthode. En d'autres termes,

24 Lors de l'instruction du dossier, la VSSE a répondu à toutes les questions du Comité et lui a fourni tous les documents demandés.

le recueil direct est le recueil au cours duquel la personne concernée donne, révèle ou communique elle-même directement les informations qui sont captées par le service de renseignement. Cela ne vise donc pas les situations dans lesquelles des données la concernant sont recueillies auprès d'un tiers.

Lors de l'évaluation préjudicielle, la portée de la saisine est quant à elle plus générale vu que sont visées toutes les méthodes particulières de recueil de données mises en œuvre ayant donné lieu à la communication d'un procès-verbal déclassifié de la Commission BIM sur la base de l'article 19/1 L.R&S.

Il résulte de cette différence que pour un même dossier d'enquête de renseignement ayant été judiciarisé, la portée du contrôle du Comité n'est pas nécessairement la même selon qu'il est saisi d'une plainte ou d'une demande d'avis préjudiciel.

Concurrence entre une enquête pénale et une enquête de renseignement

Le Comité a également confirmé qu'une enquête de renseignement peut être menée par les services de renseignement et de sécurité parallèlement à une enquête judiciaire menée par les autorités judiciaires.

Même si les services de renseignement et de sécurité sont obligés de dénoncer à la Commission BIM la prise de connaissance de certains indices ou faits, la finalité d'une enquête d'un service de renseignement reste la collecte de renseignements liés aux missions légales des services de renseignement et de sécurité.

Les articles 13/5 et 19/1 de la L.R&S prévoient des dispositions réglant l'interaction entre une enquête de renseignement et une enquête pénale. L'article 13/5 de la L.R&S ne peut pas s'interpréter comme conférant aux enquêtes pénales une préséance sur les enquêtes de renseignement ou comme interdisant la conduite simultanée de ces deux types d'enquêtes. Cet article laisse au contraire envisager de nombreuses hypothèses dans lesquelles une enquête de renseignement se poursuit en parallèle d'une enquête judiciaire.

L'article 19/1 L.R&S encadre également les conséquences d'une dénonciation de certains indices ou faits par les services de renseignement et de sécurité auprès de la Commission BIM. Les conséquences relatives à la valeur probante d'un procès-verbal déclassifié doivent être appréciées par les juridictions pénales et non par le Comité.

Le Comité peut vérifier qu'il n'y a pas eu de manquement dans le chef des services de renseignement et de sécurité par rapport à ces deux articles. Par contre, le Comité est incompétent pour contrôler le travail de la Commission BIM dont l'indépendance est garantie dans la loi.

Enfin, le Comité considère qu'un éventuel manquement lié à la concertation et/ou aux communications entre un service de renseignement et de sécurité et la Commission BIM d'une part et les autorités judiciaires d'autre part, n'a pas d'impact sur la légalité des méthodes.

2. LES MESURES D'APPUI

Depuis la modification législative de 2022, il est possible de solliciter des mesures d'appui. Les articles 13/1 à 13/3 de la L.R&S prévoient la commission d'infractions pénales, l'usage de faux noms ainsi que la création de personnes morales dans l'unique but d'améliorer la position d'information du service par l'intermédiaire d'un agent ou d'une source. Les mesures d'appui se distinguent des méthodes de recueil de données puisqu'à la différence de ces dernières, les mesures d'appui ne peuvent pas être utilisées pour collecter des informations. Elles doivent toutefois également être proportionnées à l'objectif poursuivi et ne peuvent en aucun cas mettre en péril l'intégrité physique des personnes lors de leur exécution. Les services recourent à ces mesures d'appui afin de protéger ou renforcer leur position d'information. Pensons, par exemple, à une source qui tient des propos pénalement répréhensibles sur internet pour démontrer sa loyauté envers un groupe extrémiste.

Les mesures d'appui sont également soumises à des règles strictes. Lorsqu'elles impliquent des faits punissables, le service demandeur doit toujours les soumettre à la Commission BIM, afin que celleci puisse se prononcer sur leur proportionnalité. Pour l'usage d'identités fictives, la transmission d'une liste mensuelle suffit.[25]

En 2025, 17 mesures demandes d'autorisation de commission d'infractions par des agents ou des sources humaines ont été autorisées par la Commission BIM. Elles ont toutes été introduites par la VSSE.

3. INTERCEPTIONS À L'ÉTRANGER, PRISES D'IMAGES ET INTRUSIONS DANS DES SYSTÈMES INFORMATIQUES

L'article 44 de la L.R&S permet au SGRS de rechercher, capter, écouter, prendre connaissance et enregistrer toute forme de communications émises ou reçues à l'étranger.

A cette fin, le SGRS est chargé d'élaborer annuellement un plan d'interceptions, un plan d'intrusions ainsi qu'un plan d'images dans lesquels il dresse « *une liste d'organisations et d'institutions qui feront l'objet d'interceptions de leurs communications, d'intrusions dans leurs systèmes informatiques ou de prises d'images fixes ou animées dans le courant de l'année à venir. Ces listes justifieront pour chaque organisation ou institution la raison pour laquelle elle fera l'objet d'une interception, intrusion ou prise d'images fixes ou animées en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°, et mentionneront la durée prévue* » (art. 44/3 L.R&S).

Ces compétences sont soumises à un triple contrôle du Comité, préalablement, pendant et après l'exécution des interceptions, intrusions ou prises d'images. Le contrôle *préalable* s'effectue sur la base des listes établies annuellement par le SGRS et soumises à l'autorisation du ministre de la Défense. Le contrôle réalisé *pendant* l'interception, l'intrusion ou la prise d'images s'effectue « *à tout*

25 À propos des missions attribuées à ce propos au Comité R/I, voy. Comité R/I, *Rapport d'activités 2022*, pp. 86-87.

moment moyennant des visites aux installations dans lesquelles le Service Général du Renseignement et de la Sécurité effectue ces interceptions, intrusions et prises d'images fixes ou animées ». Le contrôle réalisé *après* l'exécution s'effectue sur la base de listes mensuelles des pays ou des organisations ou institutions ayant effectivement fait l'objet d'une écoute, d'une intrusion ou d'une prise d'images ainsi que sur la base du contrôle de journaux de bord tenus de façon permanente sur le lieu d'interception, d'intrusion ou de prise d'images.

Le Comité R/I a réceptionné les trois plans pour l'année 2025 dans le courant du mois de décembre 2024, après qu'ils aient été approuvés, comme le prévoit la L.R&S, par le ministre de la Défense.

En 2025, le Comité a effectué une série de visites sur site ainsi que plusieurs réunions avec le SGRS qui lui ont permis de collecter des informations complémentaires sur la manière dont cette mission est exercée par le SGRS.

Le Comité a également remis en 2025 un avis concernant un projet d'arrêté royal fixant certaines règles relatives l'exercice de cette compétence.

PLAINTES, DÉNONCIATIONS ET REQUÊTES

IDENTIFIER, COMPRENDRE ET CORRIGER LES DYSFONCTIONNEMENTS

Le Comité R/I examine les plaintes, dénonciations et requêtes individuelles des citoyens en vertu de l'article 34 de la L.Contrôle. Celles-ci sont classées en trois catégories :

- les **plaintes 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 ;
- les **plaintes relatives à l'utilisation de méthodes particulières de renseignement** (MPR) par la VSSE ou le SGRS ;
- les **requêtes individuelles relatives aux traitements de données à caractère personnel** par les services susmentionnés, leurs membres ainsi que leurs sous-traitants. Le Comité R/I agit en cette matière 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 (les plaintes dites DPA[26]).

1. APERÇU CHIFFRÉ

En 2025, le Comité R/I a reçu, au total, **63 plaintes, dénonciations et requêtes**.

Les colonnes du tableau ci-dessous les ventilent selon que la compétence du Comité R/I est exclusive ou conjointe avec le Comité P ou l'Organe de contrôle de l'information policière (C.O.C.).[27]

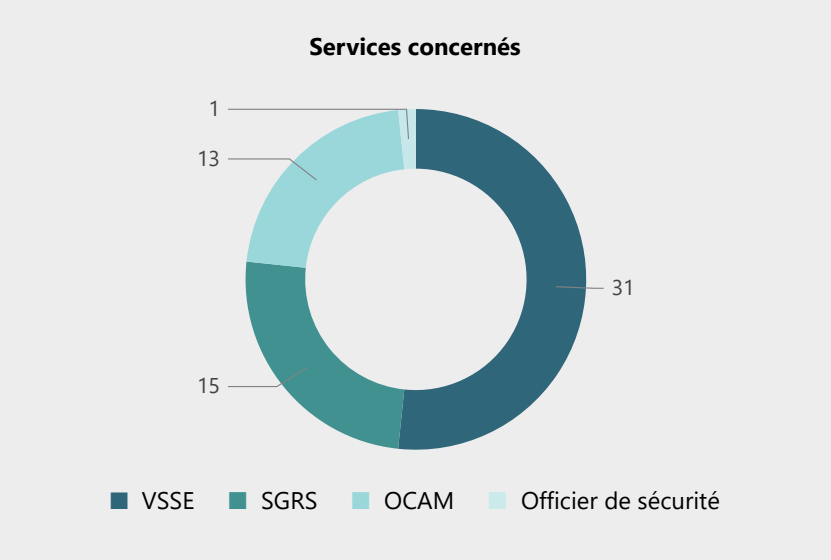
2025	COMITÉ R/I	COMITÉ R/I et COMITÉ P	COMITÉ R/I et C.O.C.	TOTAL
Plaintes introduites	58	3	2	63
Plaintes irrecevables	20	1	0	21
Plaintes recevables	38	2	2	42
Dossiers en suspens	0	0	0	0
Dossiers en cours	3	0	0	3
Dossiers recevables clôturés	35	2	2	39
Mesures correctives	4	1	0	5

26 DPA signifie *Data Protection Authority*.

27 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 R/I et P (pour le volet OCAM de l'enquête) et dans les dossiers traités exclusivement par le Comité R/I (pour les devoirs d'enquêtes portant sur la VSSE).

61 plaintes ont pu être clôturées en 2025. Seul un nombre limité de plaintes était toujours en cours de traitement début 2026. Après une brève pré-enquête et la vérification de plusieurs données objectives, le Comité a rejeté 21 plaintes et dénonciations parce qu'elles étaient manifestement irrecevables, ou parce que le Comité n'était pas compétent pour en traiter les griefs. En comparaison aux années précédentes, on observe une **légère augmentation du nombre de plaintes recevables** soumises au Comité R/I.

Pour être recevable, une plainte ou une dénonciation doit concerner un ou plusieurs des services soumis à contrôle. Si les plaintes portent sur des interventions policières ou le fonctionnement de la justice, les plaignants sont, si possible, renvoyés vers les instances compétentes (par exemple, le Conseil supérieur de la justice, le ministère public, le C.O.C. ou le Comité P). Si les dénonciations ne contiennent que des informations utiles susceptibles d'intéresser les services de renseignement en première ligne, celles-ci leur sont transmises. Le Comité n'est pas compétent pour examiner les plaintes concernant le fonctionnement des services de renseignement étrangers sur le territoire belge. Les plaintes relatives au fonctionnement et/ou aux décisions des Task forces locales (TFL) et des Cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme (CSIL-R) sont également irrecevables, sauf si elles portent sur les contributions des services de renseignement et de sécurité au sein de ces instances. En outre, une plainte ou une dénonciation est recevable si le plaignant ou le dénonciateur présente une pièce d'identité dans les trente jours. Les plaintes anonymes ne sont pas traitées, mais l'identité peut être protégée si le plaignant le souhaite (sauf dans le cas des plaintes DPA où l'identité est déterminante pour les vérifications auprès des services de renseignement).



L'aperçu des services visés par les plaintes déposées en 2025 montre que la VSSE est très fortement représentée.

2. NATURE DES PLAINTES RECEVABLES

Parmi les 42 plaintes recevables, 23 portaient sur des dysfonctionnements de service(s), et 18 concernaient des requêtes individuelles relatives aux traitements de données à caractère personnel (plaintes DPA). Aucune plainte ne concernait l'utilisation de méthodes particulières de renseignement par les services de renseignement.

2025	COMITÉ R/I	COMITÉ R/I et COMITÉ P	COMITÉ R/I et C.O.C.	TOTAL
Plaintes visant des dysfonctionnements	23	1	0	24
Plaintes MPR	0	0	0	0
Plaintes DPA	15	1	2	18

2.1. Plaintes visant des dysfonctionnements des services

Parmi les 24 plaintes concernant le fonctionnement, l'intervention, l'action ou l'absence d'action des services de renseignement, de l'OCAM et de ses services d'appui et de leurs membres, **seules trois ont été jugées fondées**.

Dans chacun de ces trois dossiers, des **mesures concrètes** ont été prises par les services **pour remédier au problème de fonctionnement identifié**. Deux plaintes concernaient des dossiers dans lesquels un recours contre le refus d'une habilitation de sécurité avait été introduit auprès de l'Organe de recours et où la révision de la décision n'avait pas été effectuée. Un autre dossier concernait un candidat classé favorablement par un service de renseignement qui, en raison d'une erreur matérielle, n'avait jamais été appelé à prendre ses fonctions.

Les 21 autres plaintes non fondées étaient très diverses. Il a été constaté que certains dossiers comportaient une procédure civile, disciplinaire ou pénale sous-jacente, qui dépassait la compétence du Comité. Dans deux dossiers où les plaignants étaient mis en cause dans une affaire judiciaire, ceux-ci affirmaient – à tort – qu'ils avaient travaillé pendant des années comme « informateurs » d'un service de renseignement et qu'à ce titre, ils avaient droit à une forme d'immunité pénale. De nombreuses personnes ont par ailleurs estimé faire l'objet d'une surveillance continue de la part des services de renseignement, que ce soit par des agents physiques présumés dans leur entourage (observation) ou par influence cognitive. Après enquête, aucune de ces plaintes n'a pu être jugée fondée.

2.2. Plaintes DPA

Parmi les 18 plaintes DPA que le Comité a eu à traiter figuraient plusieurs requêtes déposées dans le cadre d'une **demande d'obtention de la nationalité ou d'un titre de séjour**. Confrontés à une décision négative motivée sur la base d'informations fournies par la VSSE, le SGRS et/ou l'OCAM, les requérants s'adressent (entre autres) au Comité R/I pour un contrôle du traitement de leurs données à caractère personnel. La manière dont ces données ont été et sont partagées avec des partenaires

étrangers attirent également de plus en plus l'attention du Comité, qui est saisi par des requérants rencontrant des problèmes lors d'un contrôle aux frontières. Il n'est pas rare qu'il s'agisse de personnes qui ont été connues par le passé dans le cadre du terrorisme, de l'extrémisme ou de la radicalisation, mais pour lesquelles aucune information actualisée ne circule plus et qui ne font plus l'objet d'un suivi. En raison de la prolifération mondiale des listes de noms après les attentats, certaines personnes figurent sur des listes étrangères et en subissent les conséquences. Le Comité n'a toutefois aucune compétence vis-à-vis des services de renseignement étrangers et peut uniquement demander à la VSSE et au SGRS d'informer leurs services partenaires étrangers. En d'autres termes, il dépend de la bonne volonté de ces services, étant entendu que la coopération avec ceux-ci est parfois limitée, voire inexistante.

En 2025, le Comité R/I a examiné pour la première fois une plainte DPA contre un **officier de sécurité d'un organisme de contrôle fédéral indépendant**, qui n'avait aucun lien avec les services de renseignement et de sécurité. Toutefois, à la suite d'une récente modification législative, le Comité R/I est devenu compétent à titre résiduel pour toutes les plaintes DPA visant des officiers de sécurité, tant dans le secteur public que dans le secteur privé.

En sa qualité d'autorité de contrôle, le Comité R/I a ordonné **des mesures correctives dans deux dossiers** (art. 51/3 L.Contrôle) Le Comité ne peut toutefois pas se substituer aux services en ce sens qu'il ne peut pas effectuer lui-même une analyse des renseignements, mais il peut rendre des décisions contraignantes lorsqu'il a jugé qu'un traitement de données à caractère personnel était illégal. Selon le dossier, il peut s'agir d'exiger la rectification ou la suppression de données à caractère personnel, de porter la décision du Comité R/I à la connaissance des partenaires et/ou des autorités, ou encore de diffuser la décision au sein du service concerné.

AVIS

UN ÉVENTAIL VARIÉ MAIS COHÉRENT DE POSITIONS JURIDIQUES

Le Comité R/I 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). Le Comité doit par ailleurs 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). Il arrive que des avis soient formulés à partir de cette double compétence.

En 2025, **le Comité a été sollicité à quatre reprises** : deux fois par le ministre de l'Intérieur, une fois par le ministre de la Défense ainsi qu'une fois par la Chambre des représentants. Le délai moyen pour rendre un avis est de deux mois.

Sont repris ci-dessous un résumé des avis rendus. Les principaux arguments avancés y sont brièvement présentés. Il convient de se reporter à l'intégralité des avis pour en saisir pleinement la portée et la cohérence.[28]

1. CONCERTATION ORGANISÉE SUR LA BASE DE L'ARTICLE 458*TER* DU CODE PÉNAL

L'article 458*ter* du Code pénal dispose que :

> *« § 1er. Il n'y a pas d'infraction lorsqu'une personne qui, par état ou par profession, est dépositaire de secrets, communique ceux-ci dans le cadre d'une concertation organisée soit par ou en vertu d'une loi, d'un décret ou d'une ordonnance, soit moyennant une autorisation motivée du procureur du Roi. Cette concertation peut exclusivement être organisée soit en vue de protéger l'intégrité physique et psychique de la personne ou de tiers, soit en vue de prévenir les délits visés au Titre Ie ter du livre II ou les délits commis dans le cadre d'une organisation criminelle, telle qu'elle est définie à l'article 324bis. La loi, le décret ou l'ordonnance, ou l'autorisation motivée du procureur du Roi, visés à l'alinéa 1er, déterminent au moins qui peut participer à la concertation, avec quelle finalité et selon quelles modalités la concertation aura lieu.*

28 L'ensemble des avis sont consultables sur le site internet du Comité (www.comiteri.be).

§ 2. Les participants sont tenus au secret relativement aux secrets communiqués durant la concertation. Toute personne violant ce secret sera punie des peines prévues à l'article 458. Les secrets qui sont communiqués pendant cette concertation ne peuvent donner lieu à la poursuite pénale que des seuls délits pour lesquels la concertation a été organisée. »

Insérée par la Loi du 6 juillet 2017 dite Loi Pot-Pourri V[29], cette disposition permet de communiquer des informations (protégées) dans le cadre d'une concertation confidentielle avec les services de police ou à la demande du procureur du Roi, lorsqu'il s'agit de protéger l'intégrité physique ou mentale d'une personne ou de tiers ou de protéger la sécurité publique. Sont notamment visées par cette disposition les concertations ayant lieu dans le cadre des Cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme (CSIL). Des données à caractère personnel étant traitées dans le cadre de ces concertations, une base juridique spécifique pour encadrer ces traitements était nécessaire.

Le 12 novembre 2024, une **proposition de loi** relative au traitement de données à caractère personnel lors de la participation à une concertation organisée sur la base de l'article 458*ter* du Code pénal a été déposée à la Chambre des représentants. Par l'intermédiaire de l'Autorité de protection des données (APD), le Comité a été saisi pour rendre un avis sur le texte.

Dans son avis, rendu **le 25 février 2025**, le Comité a relevé que la proposition manquait de clarté concernant les autorités précisément visées. A défaut de disposition désignant formellement des autorités du Titre 3 de Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD)[30], le Comité R/I a jugé que le texte ne s'appliquait pas aux autorités à l'égard desquelles il est l'autorité de contrôle compétente en matière de protection des données, et par conséquent qu'il n'était pas compétent pour remettre un avis. Il ajoutait néanmoins qu'à considérer que l'intention des auteurs était de viser certaines autorités du Titre 3 de la LPD, alors le dispositif de la proposition devait être explicitement complété en ce sens et les éléments essentiels des traitements réglés. A défaut, et en l'absence de ces éléments, la proposition mettait à mal le principe de légalité.

Le 18 juin 2025, l'auteur déposait une nouvelle version du texte à la Chambre clarifiant un certain nombre de points.[31] La proposition a été adoptée en séance plénière le 8 janvier 2026.

29 Loi du 6 juillet 2017 portant simplification, harmonisation, informatisation et modernisation de dispositions de droit civil et de procédure civile ainsi que du notariat, et portant diverses mesures en matière de justice, *M.B.* 24 juillet 2017.

30 Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.* 5 septembre 2018.

31 Proposition de loi relative au traitement de données à caractère personnel lors de la participation à une concertation organisée sur la base de l'article 458*ter* du Code pénal, *Doc.Parl.*, Chambre des représentants, 2024-2025, Doc 56 0935/001, 18 juin 2025.

2. INTERCEPTION DES COMMUNICATIONS À L'ÉTRANGER PAR LE SGRS

Le SGRS peut rechercher, capter, écouter, prendre connaissance et enregistrer toute forme de communications émises ou reçues à l'étranger pour l'exécution de ses missions. Les articles 44 à 44/5 de la Loi organique des services de renseignement et de sécurité (L.R&S) reprennent les dispositions particulières à l'exercice de cette compétence ainsi que les modalités relatives au contrôle exercé en la matière par le Comité R/I.

Le 28 juillet 2025, le Comité a été saisi par le **ministre de la Défense** pour rendre un avis sur un projet d'arrêté royal fixant les règles de destruction des données illégalement recueillies visées à l'article 44/4 de la L.R&S et fixant les règles de coopération visées à l'article 44/5 de la L.R&S.

Le projet d'arrêté royal soumis pour avis visait, comme son titre l'indique, à préciser certaines modalités d'exécution et de contrôle, à savoir :

- les règles pour la destruction de données illégalement recueillies lors de ce type d'interceptions (article 44/4 L.R&S) ;
- les règles applicables dans les cas où la coopération d'un opérateur de réseau ou d'un fournisseur de service est nécessaire pour permettre une interception (article 44/5 L.R&S). Le projet visait à encadrer, par des restrictions et garanties, les flux de données et métadonnées interceptés de la sorte.

Dans son avis, rendu **le 11 septembre 2025**, le Comité formulait un certain nombre de remarques notamment concernant la destruction des données recueillies illégalement. A cet égard, il saluait le rôle central attribué au délégué à la protection des données (DPO) dans la procédure de destruction et appelait le législateur à attribuer au DPO un rôle similaire dans le cadre de la procédure de destruction des données illégalement recueillies par une méthode de renseignement particulière. Afin de permettre au Comité d'exercer son contrôle pleinement, il plaidait pour l'ajout d'une disposition imposant au SGRS de transmettre, dans un délai de deux semaines, tout procès-verbal de destruction de données recueillies illégalement. Quant aux règles applicables aux interceptions nécessitant le concours des fournisseurs de services ou des opérateurs du réseau, il appelait à mieux définir certaines notions mobilisées (telles que « transmission automatique de flux de données et métadonnées » et « directeur des opérations ») ainsi qu'à préciser certains délais dans la procédure. Par ailleurs, le Comité rappelait que tout système ou équipement utilisé par un service de renseignement pour le traitement automatisé de données à caractère personnel doit satisfaire techniquement à l'exigence d'explicabilité (principe d'*explainability*).[32]

32 La collecte d'informations au moyen d'un flux automatisé de (méta)données exige de pouvoir expliquer, tant en amont qu'en aval, la manière dont le système est parvenu à un résultat déterminé.

3. INTERDICTION ADMINISTRATIVE D'ORGANISATIONS

Par courrier du 31 juillet 2025, le Comité R/I a été saisi par une demande d'avis du **ministre de l'Intérieur** concernant un avant-projet de loi relatif à l'interdiction administrative des personnes morales, des sociétés sans personnalité juridique, des associations ou groupements de fait constituant une menace grave et actuelle pour la sécurité nationale ou la pérennité de l'ordre démocratique et constitutionnel.

L'avant-projet de loi avait pour objet de créer un mécanisme d'interdiction administrative visant les organisations qui, par leurs activités concrètes, coordonnées et persistantes, constituent une menace grave et actuelle pour la sécurité nationale ou les fondements de l'État de droit. Le projet prévoyait que l'interdiction puisse prendre deux formes : la dissolution administrative de l'organisation ou une interdiction de ses activités.

Dans son avis, remis **le 9 octobre 2025**, le Comité s'est cantonné à discuter des éléments concernant les activités et obligations des services de renseignement.[33]

En ce qui concerne les motifs pouvant conduire à une interdiction administrative, le Comité relevait notamment que le projet de loi se limitait à trois menaces pour la sécurité nationale, à savoir le terrorisme, l'extrémisme violent et le radicalisme violent, alors que la L.R&S reprend plusieurs menaces explicites pour la sécurité nationale.[34] Le Comité s'interrogeait sur le choix opéré de limiter le champ d'application à ces trois menaces et invitait l'auteur à en préciser les motifs. Le Comité invitait par ailleurs l'auteur à préciser le sens de ces trois notions non définies dans le projet. Il attirait également l'attention sur la différence de fond qui existe entre la notion de « radicalisme » d'une part, et les notions de « processus de radicalisation » et de « radicalisation » d'autre part. La première étant un état ; les dernières un processus, un parcours.

Concernant la procédure, le Comité notait le rôle prépondérant attribué au Comité de coordination du renseignement et de la sécurité (CCRS) qui se voyait confier comme nouvelle mission celle de réaliser une analyse servant de base à une éventuelle interdiction administrative. Le Comité soulevait plusieurs questions découlant de l'attribution de cette nouvelle mission formelle. Notamment celle de savoir dans quelle mesure les règles de fonctionnement existantes du CCRS devront être adaptées pour l'exécution de cette mission, mais aussi celle de savoir si le CCRS dispose des compétences suffisantes pour mener à bien cette mission et si son cadre légal devrait être adapté. Le Comité recommandait de fixer dans le projet de loi les règles relatives au quorum et à la majorité requise pour prendre une décision formelle en collège lorsqu'une analyse ou un rapport est rendu dans le cadre de ladite procédure. Le Comité relevait également que le projet était muet concernant les travaux préalables à la rédaction d'une analyse par le CCRS. Par travaux préalables, sont visés l'obtention des informations nécessaires auprès des services opérationnels compétents (par exemple la VSSE ou le SGRS) et l'analyse conjointe de ces informations par les membres du CCRS afin de pouvoir procéder

33 Pour une portée plus générale, voy. notamment les avis du Conseil d'Etat (janvier 2026) et de l'institut fédéral pour la protection et la promotion des droits humains (IFDH) (septembre 2025).

34 A savoir l'espionnage, le terrorisme, l'extrémisme, la prolifération, les organisations sectaires nuisibles, les organisations criminelles et l'ingérence (article 8, 1°, alinéa 2 L.R&S).

à l'élaboration et l'approbation d'une analyse. Le Comité relevait pourtant de nombreux points à clarifier à cet égard, tels que l'identité du service chargé réellement de l'analyse ou la marche à suivre si le CCRS estime ne pas être en possession d'informations suffisantes pour prendre une décision.

Enfin, concernant la possibilité de recours, le projet prévoyait le contrôle juridictionnel par la possibilité d'un recours contre toute interdiction administrative devant le Conseil d'Etat. A cet égard, le Comité rappelait la jurisprudence constante de la Cour européenne des droits de l'homme relative aux exigences applicables lorsque les pouvoirs publics utilisent des informations classifiées/secrètes dans une décision administrative individuelle : la Cour reconnait que, pour des raisons de sécurité nationale, l'accès d'une personne à son dossier puisse être limité, mais qu'un juge ou une autre autorité indépendante doit avoir accès à l'intégralité du dossier, y compris à tous les documents classifiés ou secrets, afin qu'une procédure de recours juridictionnel soit conforme au droit à un procès équitable (art. 6 CEDH) et au droit à un recours effectif (art. 13 CEDH). La question essentielle qui risquait de se poser aux yeux du Comité dans le cadre du recours juridictionnel prévu dans le projet, porte sur l'accès par la juridiction saisie aux pièces classifiées qui ont fondé l'avis du CCRS et partant, la décision attaquée. Le Comité relevait que la procédure de recours devant le Conseil d'Etat décrite dans le projet pourrait ne pas satisfaire aux exigences énoncées par la Cour européenne dans les cas où l'analyse du CCRS est fondée sur des informations classifiées. Si l'analyse du CCRS est basée sur des informations classifiées émanant d'un service de renseignement, et même si ce dernier a choisi de remettre une note non classifiée au CCRS, le dossier sous-jacent restera classifié. La décision prise par le CCRS reposera donc sur des informations classifiées auxquelles la juridiction appelée à statuer devrait avoir accès pour satisfaire aux exigences de la Cour européenne. Pourtant, le projet ne prévoit rien à cet égard. Pour remédier à cette lacune fondamentale, la piste à privilégier pour le Comité est de lui confier cette mission au regard des prérogatives que la loi lui attribue et de son domaine d'expertise.

Début 2026, le ministre de l'Intérieur annonçait que le projet serait revu sur la base des divers avis formulés.

4. LES LISTES PNR ET ETIAS

Le 15 septembre 2025, le Comité a été saisi par le **ministre de l'Intérieur** pour rendre un avis sur deux projets d'arrêté royal établissant, d'une part, un cadre de référence pour les finalités du traitement des données des passagers (*Passenger name record*, PNR) et, d'autre part, un cadre de référence pour la consultation des données *European Travel Information and Authorisation System* (ETIAS) à des fins répressives.

Les projets visaient à établir, en exécution de dispositions légales, des listes d'infractions en droit national qui correspondent aux infractions visées par le législateur européen. Pour le traitement de données des passagers, il s'agit des infractions terroristes et des formes graves de criminalité telles que définies à l'article 3, points 8 et 9, de la directive PNR.[35] Pour les données ETIAS, il s'agit des

35 Directive 2016/681 du Parlement européen et du Conseil européen du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

infractions terroristes et des infractions pénales graves, telles que définies à l'article 3, points 15 et 16, du règlement ETIAS.[36] L'objectif de ces deux listes était de fournir aux autorités compétentes et services opérationnels un cadre de référence afin de garantir le respect des finalités de traitement des données.

Dans son avis, rendu **le 18 novembre 2025**, le Comité R/I rappelait la restriction générale fixée par le législateur européen : pour qu'une infraction pénale puisse être inscrite sur la liste PNR ou la liste ETIAS, l'infraction doit être punie d'une peine ou d'une mesure privative de liberté d'une durée maximale d'au moins trois ans. Pour le reste, il relevait que le législateur européen avait posé peu (ou pas) de restrictions de fond pour l'interprétation à donner à certaines notions. Par conséquent, le Comité relevait que l'auteur avait adopté une interprétation restrictive de certaines notions (notamment celle d'une participation à une organisation criminelle) et qu'un certain nombre d'infractions pénales pouvaient par conséquent être ajoutées à ces deux listes. En outre, concernant la définition retenue dans l'un des projets pour la notion de sabotage, le Comité faisait remarquer que le caractère intentionnel de l'acte dans le chef de son auteur devait y être ajouté.

36 Règlement 2018/1240 du Parlement européen et du Conseil européen du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages.

LA CELLULE INTÉGRITÉ

CANAL DE SIGNALEMENT EXTERNE POUR LES ATTEINTES À L'INTÉGRITÉ

1. LA LOI SUR LES LANCEURS D'ALERTE

Les abus ou pratiques frauduleuses dans un cadre professionnel – lesdites atteintes à l'intégrité – peuvent faire l'objet d'un signalement. Les auteurs de ces signalements, également appelés « lanceurs d'alerte », jouent un rôle important en dénonçant les fraudes et irrégularités constatées au sein d'institutions publiques (ou d'entreprises privées). Cependant, la crainte de représailles peut dissuader les lanceurs d'alerte de franchir le pas et de signaler les faits. Les lanceurs d'alerte méritent donc une reconnaissance, un soutien et une protection appropriés, car ils s'exposent potentiellement à des risques professionnels et personnels considérables.[37]

Une directive européenne[38] offre une protection à ceux qui signalent ou divulguent de telles violations de la législation ou des atteintes présumées de l'intégrité. Cette directive a été transposée en droit national par 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 (Loi sur les lanceurs d'alerte).[39] La loi est entrée en vigueur le 2 janvier 2023. Agir en tant que lanceur d'alerte est donc devenu un droit et les auteurs de signalement peuvent se prévaloir de certaines normes minimales prévues pour leur protection lorsqu'ils craignent que leur signalement puisse avoir des conséquences néfastes sur leur situation (professionnelle).

La loi oblige les autorités publiques à mettre en place un système de signalement pour les lanceurs d'alerte à différents niveaux : un auteur de signalement doit avoir la possibilité de signaler un fait en interne, au sein de sa propre organisation, ou en externe. L'auteur peut également opter pour une divulgation publique.[40] Ces trois niveaux ne sont pas hiérarchisés les uns par rapport aux autres. Le choix du niveau appartient pleinement au lanceur d'alerte et n'est pas soumis au principe de subsidiarité.

La protection et le soutien offerts s'appliquent aux différents modes de signalement et impliquent une variété de mesures.[41] Les mesures de représailles sont par ailleurs interdites et un lanceur d'alerte peut bénéficier d'informations et de conseils (tant techniques que juridiques), d'un soutien psychologique et d'une assistance juridique. La loi établit une procédure qui précise le déroulement d'un signalement interne ou externe.

Dans le cadre de signalements potentiels d'atteintes à l'intégrité commises au sein du SGRS ou de la VSSE, le Comité R/I a été chargé d'agir en tant que canal de signalement externe.[42]

37 Institut fédéral pour la protection et la promotion des droits humains (IFDH), *Guide pour les lanceurs d'alerte*, décembre 2024, https://federaalinstituutmensenrechten.be/fr/publications/guide-pour-les-lanceurs-dalerte, consulté le 3 mars 2026.

38 Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, *Journal officiel de l'Union européenne*, 26 novembre 2019, L305/17.

39 *M.B.*, 23 décembre 2022.

40 Art. 7, § 1er, 2° de la Loi sur les lanceurs d'alerte.

41 Art. 28 et art. 29 de la Loi sur les lanceurs d'alerte.

42 Art. 14, § 1er, alinéa 3 de la Loi sur les lanceurs d'alerte.

2. LA CELLULE INTÉGRITÉ AU SEIN DU COMITÉ R/I

Dans le cadre de l'exécution de sa mission en tant que canal de signalement externe pour les atteintes à l'intégrité commises au sein du SGRS et de la VSSE, la Cellule Intégrité a été créée au sein du Comité R/I. Celle-ci a été constituée dans le respect de la parité linguistique ainsi que d'une représentation équilibrée entre hommes et femmes. La cellule se compose de quatre collaborateurs du Comité R/I : deux commissaires-auditeurs (Service d'Enquêtes) et deux juristes (Section juridique).

Les collaborateurs ou membres du SGRS ou de la VSSE peuvent désormais s'adresser au Comité R/I pour signaler une atteinte (présumée) à l'intégrité. La Cellule Intégrité mènera une enquête afin de vérifier si le signalement est recevable et fondé, et de déterminer ce qui peut/doit être fait pour mettre fin à l'atteinte ou pour éviter qu'elle ne se reproduise à l'avenir.

À cette fin, la Cellule dispose d'un large éventail de compétences et de moyens d'enquête : les personnes concernées peuvent être invitées à apporter leur collaboration et être entendues, les pièces utiles peuvent être sollicitées… Cette mission en tant que canal de signalement externe implique non seulement de nombreuses compétences en matière d'enquête sur l'atteinte potentielle à l'intégrité, mais aussi une responsabilité quant à la protection contre les représailles de l'auteur du signalement et des personnes qui coopèrent à l'enquête.[43] Les membres de la Cellule Intégrité ont suivi, fin 2024-début 2025, une formation spécifique en vue du traitement des signalements.[44]

Fin 2025, le Centre Intégrité du Médiateur fédéral a initié la création d'un réseau informel réunissant les différents canaux de signalement externes du secteur public auquel les membres de la Cellule Intégrité participent. Il s'agit d'un groupe d'échange informel visant à rassembler des experts des différents canaux concernés afin d'échanger sur les enjeux et défis communs auxquels leurs services sont confrontés. Une première réunion de lancement s'est tenue en janvier 2026. Le réseau devrait se réunir trois à quatre fois par an. Le réseau vise notamment à renforcer les liens entre les canaux de signalement externes, à partager des connaissances et bonnes pratiques, à améliorer leur visibilité ou encore à affirmer leur rôle stratégique dans la protection des lanceurs d'alerte au sein du secteur public.

43 Art. 14, § 1er, 6° de la Loi sur les lanceurs d'alerte.

44 Art. 14, § 2 de la Loi sur les lanceurs d'alerte. Il s'agissait de la formation « *Masterclass Fraud Auditing* » dispensée par *l'Institute of Fraud Auditors* (IFA), une formation post-master pour cadres destinée aux professionnels se spécialisant dans la lutte contre la fraude, les enquêtes et la prévention de la fraude. Elle vise à former des auditeurs en matière de fraude efficaces en leur transmettant des connaissances approfondies et des compétences pratiques en matière de gestion des risques de fraude, de prévention et d'enquête en matière de fraude, de techniques d'entretien, de cybercriminalité, d'analyse de scénarios de fraude et d'apprentissage des meilleures pratiques dans les secteurs public et privé. La formation a été suivie avec succès en 2025 par tous les membres de la Cellule Intégrité.

3. CHAMP D'APPLICATION ET SES LIMITES

3.1. Un défi important : la sécurité nationale

En tant que canal de signalement externe pour le SGRS et la VSSE, le Comité R/I enquête sur les éventuels signalements d'abus, d'irrégularités et de fraudes au sein de ces deux services de renseignement. Mais un défi important se pose dès lors que la Loi sur les lanceurs d'alerte exclut spécifiquement le domaine de la « sécurité nationale »[45] de son champ d'application bien que le fonctionnement des services de renseignement s'articule autour de la sécurité nationale. L'article 4 de la loi sur les lanceurs d'alerte stipule :

> *« § 1er. La présente loi ne s'applique pas :*
> *1° aux informations classifiées*
> *…*
> *§ 2. La présente loi ne s'applique pas au domaine de la sécurité nationale, sauf en ce qui concerne les signalements de violations des règles relatives aux marchés publics dans les domaines de la défense et de la sécurité visés à l'article 3, § 4, alinéa 1er. »*

Le SGRS et la VSSE sont des services chargés de la « sécurité nationale ».[46] L'exclusion expresse des violations susmentionnées rend particulièrement difficile – voire pratiquement impossible – la mise en œuvre effective de la Loi sur les lanceurs d'alerte dans la pratique des services de renseignement, ainsi que la concrétisation de son objectif de protection. L'exposé des motifs de la Loi sur les lanceurs d'alerte indiquait d'ailleurs déjà à l'époque, à propos de l'exclusion des violations commises lors d'activités relevant de la sécurité nationale :

> *« […] Pour ces violations, un système de signalement (interne et externe) spécifique sera créé dans une loi distincte. Dans cette loi spécifique, des garanties suffisantes seront intégrées pour assurer la nature secrète des opérations des services de renseignement et de sécurité […] »*[47]

45 Conformément à l'exposé des motifs, la « sécurité nationale » est définie ici comme « *l'ensemble des missions des services de renseignement et de sécurité visées aux articles 7 et 11 de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité* ».

46 Art. 7 et art. 11 L.R&S.

47 Projet de loi relatif 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, 3 novembre 2022, Exposé des motifs, p. 170.

Dans son avis relatif au projet de loi sur les lanceurs d'alerte dans le secteur public[48], le Comité R/I a, pour sa part, mis en garde contre une distinction difficile à manier :

> *« […] En ce qui concerne les atteintes à l'intégrité commises à l'encontre des services de renseignement, le Comité est toutefois d'avis qu'il sera impossible, dans la pratique, d'établir une distinction claire entre les atteintes à l'intégrité commises en dehors de l'exercice des missions de ces services et les atteintes à l'intégrité commises pendant l'exercice de celles-ci. […] »*

Début 2026, il convient de constater qu'il n'existe pas encore d'alternative à part entière pour la protection des auteurs de signalement d'atteintes à l'intégrité commises dans les domaines exclus par l'article 4 de la Loi sur les lanceurs d'alerte. Un projet de loi régissant le statut des lanceurs d'alerte en ce qui concerne les atteintes à l'intégrité exclues de la première loi est en cours d'élaboration.

3.2. Des signalements restent toutefois possibles…

L'absence d'un statut de protection pour les auteurs de signalement d'atteintes à l'intégrité commises dans le contexte de la sécurité nationale n'empêche toutefois pas que de tels signalements puissent être effectués.

En effet, le Comité R/I peut être saisi de différentes manières pour mener une enquête, même si cela se fait en dehors du cadre de la Loi sur les lanceurs d'alerte. Néanmoins, en l'absence d'une législation spécifique, la protection supplémentaire — qui constitue précisément une valeur ajoutée dans ce type de situations et pourrait encourager les personnes concernées à procéder effectivement au signalement — fait encore défaut.

Dans la pratique, les exclusions prévues à l'article 4 de la Loi sur les lanceurs d'alerte ont pour conséquence qu'il est actuellement très difficile pour le Comité de remplir pleinement sa mission de canal de signalement externe. Dès qu'un signalement est effectué concernant une violation commise au sein du SGRS ou de la VSSE, il porte sur des services dont la raison d'être repose sur des missions relevant de la sécurité nationale. Le Comité R/I souligne donc l'importance d'un cadre législatif complémentaire afin que les auteurs de signalement d'atteintes à l'intégrité commises au sein du SGRS ou de la VSSE puissent bénéficier du même droit à la protection et au soutien que celui prévu par la directive (*infra*), et ce sans porter atteinte à d'autres intérêts qui, en raison de leur spécificité, ne peuvent pas non plus – et à juste titre – être perdus de vue.

48 COMITE R/I, Avis n° 005/CPR/2022 du 30 août 2022 concernant le projet de loi sur la réglementation relative aux lanceurs d'alerte du secteur public (l'actuelle loi sur les lanceurs d'alerte) (www.comiteri.be).

3.3. Les mesures de protection et de soutien

Lorsqu'un lanceur d'alerte a effectué un signalement recevable, il peut bénéficier des mesures de protection prévues par la loi.[49] Celles-ci concernent principalement la protection contre les mesures de représailles. Si la personne estime être victime d'une telle mesure, elle peut introduire une plainte auprès du canal externe compétent.

Les représailles recouvrent un large éventail de formes possibles : suspension, rétrogradation, évaluation de performance négative, discrimination, coercition, intimidation… Il appartient à l'autorité publique concernée de démontrer que la mesure en question ne constitue pas une mesure de représailles à la suite du signalement. Les personnes qui assistent l'auteur du signalement et/ou ont coopéré à l'enquête peuvent également compter sur les mesures de protection et de soutien prévues, telles que la mise à disposition d'informations et de conseils, une assistance juridique, un soutien psychologique, un soutien médiatique et social…

Un signalement d'atteinte à l'intégrité n'est pas une plainte individuelle
Un lanceur d'alerte signalant une atteinte à l'intégrité occupe une position fondamentalement différente de celle d'une personne qui introduit une plainte concernant le fonctionnement de membres des services de renseignement. Alors qu'une plainte implique que le plaignant subit personnellement un préjudice du fait du comportement « fautif » d'un agent, cela ne vaut en principe pas pour les auteurs de signalements d'atteintes à l'intégrité. Un signalement peut dès lors être effectué et déclencher une enquête sans besoin d'échanges répétés avec le lanceur d'alerte.

3.4. Une atteinte à l'intégrité signalée

Les signalements adressés en 2025 au Comité R/I dans le cadre de sa mission de canal de signalement externe ont été évalués selon la législation en vigueur. Par conséquent, les seuls signalements pouvant être recevables relèvent d'activités des services de renseignement non liées à leurs missions de sécurité nationale.[50] Une donnée qui peut sembler quelque peu paradoxale. En 2025, un dossier a été ouvert et déclaré recevable concernant un signalement d'une atteinte à l'intégrité. Cette enquête est toujours en cours en 2026.

Vous êtes membre du SGRS ou de la VSSE et vous souhaitez signaler une atteinte à l'intégrité ? Vous pouvez le faire par e-mail (signalement_melding@comiteri.be), par téléphone (02/286.29.11, demandez la Cellule Intégrité) ou sur rendez-vous. Vous pouvez également introduire un signalement par écrit (Comité R/I, Cellule Intégrité, Rue de Louvain 48, boîte 5, 1000 Bruxelles).

49 Art. 28 et art. 29 de la Loi sur les lanceurs d'alerte.

50 Les signalements d'atteintes commises dans le cadre de leurs missions relevant de la sécurité nationale sont irrecevables (au titre du statut de protection prévu par la Loi sur les lanceurs d'alerte).

L'ORGANE DE RECOURS EN MATIÈRE D'HABILITATIONS ET D'AVIS DE SÉCURITÉ

UN NOMBRE RECORD DE DOSSIERS

L'Organe de recours est la juridiction administrative compétente pour connaître du contentieux en matière d'habilitations de sécurité et d'avis de sécurité. Il s'agit d'un organe collégial composé des (suppléant(e)s des) président(e)s du Comité R/I, du Comité P et de la Chambre contentieuse de l'Autorité de protection des données.

L'Organe de recours rend soit des décisions, lorsqu'il est saisi d'un recours en matière d'habilitations de sécurité, soit des avis, lorsqu'il est saisi d'un recours portant sur un avis de sécurité. Par souci de lisibilité, le terme « décisions de l'Organe de recours » sera utilisé dans le présent rapport pour désigner indistinctement les décisions et avis rendus par l'Organe de recours.

Le Comité R/I assure la présidence et le greffe de l'Organe de recours. Il met à disposition les membres du personnel et ressources nécessaires au fonctionnement de l'Organe de recours, notamment pour la tenue du greffe, l'organisation des audiences, la rédaction des procès-verbaux ou l'élaboration des décisions.

1. TENDANCES GÉNÉRALES

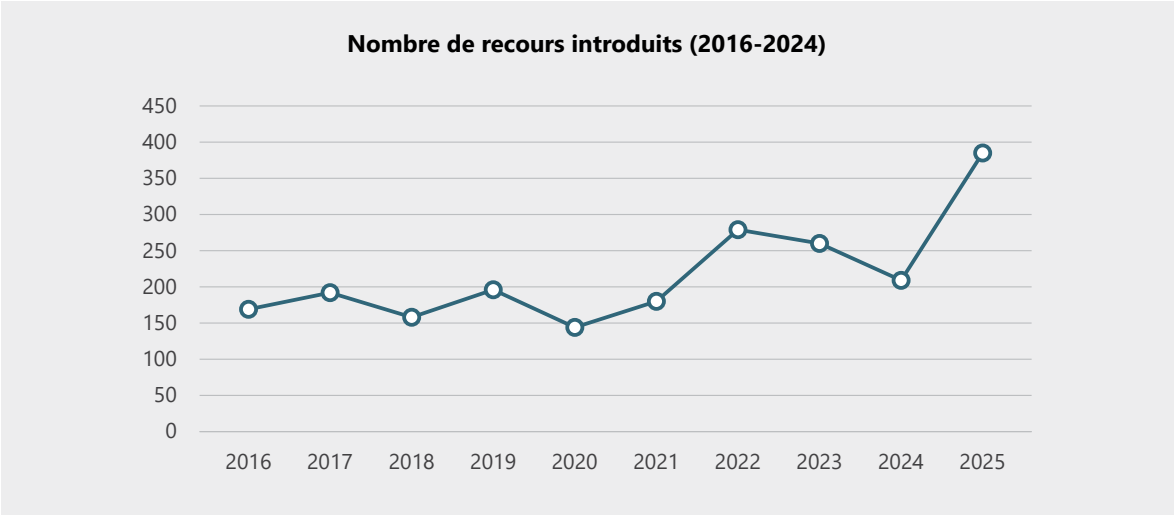
L'année 2025 a été marquée par un volume important de recours introduits et examinés par l'Organe de recours. Dans les paragraphes qui suivent, une vue d'ensemble de l'activité de l'Organe de recours est proposée. Y sont détaillés entre autres le nombre de recours introduits selon la nature des décisions contestées et la langue de la procédure, ainsi que le nombre et le type de décisions rendues par l'Organe de recours ou encore les délais de traitement observés.

Les chiffres présentés reflètent exclusivement le contentieux traité par l'Organe de recours. Ils ne rendent pas compte du volume total des décisions ou avis défavorables adoptés par les autorités de sécurité et de vérification[51] [52], dont une partie seulement fait l'objet d'un recours. Par conséquent, les tendances observées ne doivent pas être interprétées comme un indicateur direct de l'évolution de l'activité de ces autorités. Pour disposer d'une vision complète du nombre d'habilitations et d'avis de sécurité délivrés durant l'année écoulée, il convient de se référer au rapport annuel des différentes autorités compétentes.

51 Il existe trois autorités de sécurité : l'Autorité nationale de sécurité, la Sûreté de l'Etat (VSSE) et le Service Général du Renseignement et de la Sécurité (SGRS).

52 La notion 'd'autorité de vérification' désigne l'autorité qui délivre les avis de sécurité. Parmi ces autorités figurent notamment, la Police fédérale, le SGRS,...

1.1. Nombre de recours introduits en forte augmentation



	2020	2021	2022	2023	2024	2025
ANS	91	86	183	188	77	97
VSSE	0	4	2	0	1	3
SGRS	41	84	76	56	65	88
AFCN	7	6	12	11	10	14
Police fédérale	4	0	1	4	56	182
Police locale	1	0	5	1	0	1
TOTAL	**144**	**180**	**279**	**260**	**209**	**385**

En 2025, le nombre de recours introduits a connu une hausse significative, passant de 209 en 2024 à 385 en 2025, ce qui représente une augmentation de 84%. Cette augmentation concerne principalement les recours dirigés contre des avis de sécurité, même si les recours en matière d'habilitations de sécurité ont également connu une progression notable (cf. ci-dessous).

L'évolution est également marquée par une augmentation du nombre de recours selon la langue de la procédure. Les recours introduits en néerlandais ont enregistré la croissance la plus importante, passant de 76 recours en 2024 à 195 recours en 2025, soit une augmentation de 156% (voir *infra*). Les recours introduits en français poursuivent quant à eux une progression régulière, passant de 133 recours en 2024 à 190 recours en 2025, soit une augmentation de 43%.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Français	99	115	83	101	83	86	201	159	133	190
Néerlandais	70	77	75	95	61	94	123	101	76	195
Allemand	0	0	0	0	0	0	0	0	0	0

1.2. Répartition des recours selon la nature des décisions contestées

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Habilitations	50	40	36	51	32	60	83	105	102	145
Avis	101	122	92	115	99	108	157	134	85	234
Attestations	18	30	30	30	13	12	39	21	22	6
TOTAL	**169**	**192**	**158**	**196**	**144**	**180**	**279**	**260**	**209**	**385**

1.2.1. Habilitations de sécurité

En 2025, le nombre de recours introduits relatifs à des habilitations de sécurité a fortement augmenté, passant de 102 dossiers en 2024 à 145 dossiers, soit une hausse de 42 %. L'Organe de recours ne dispose pas des éléments permettant de déterminer la cause de l'augmentation du nombre de recours. Il est à noter que 23% de ces recours (33 sur 145) ont été introduits en raison d'une absence de décision (ou de sa notification au requérant) par l'autorité de sécurité dans le délai légal.

1.2.2. Avis de sécurité

Les avis de sécurité ont connu l'évolution la plus marquée, avec 234 recours en 2025 contre 85 en 2024, soit une augmentation de 175%. Cette augmentation est essentiellement liée aux recours introduits contre un avis de sécurité négatif pour exercer une fonction dans une enceinte portuaire. Le screening de sécurité pour l'accès aux ports, obligatoire depuis 2024, explique en grande partie cette progression. Compte tenu de la situation géopolitique, il est probable que les screenings deviennent plus stricts, ce qui pourrait entraîner une hausse des avis de sécurité négatifs et, par conséquent, des recours introduits.

Par ailleurs, l'abrogation des attestations de sécurité (abordée *infra*) a également contribué à l'évolution du nombre d'avis de sécurité rendus, un avis étant désormais exigé pour les fonctions et secteurs qui nécessitaient auparavant une attestation.

1.2.3. Attestations de sécurité

Le système des attestations de sécurité ayant été abrogé (voir *infra*), plus aucune attestation n'est délivrée depuis le 1er février 2025. Cette réforme a logiquement entraîné une diminution du nombre de recours introduits en la matière. L'Organe de recours a toutefois encore traité six dossiers en 2025 portant sur des refus d'attestations de sécurité intervenus avant l'abrogation de ce régime.

1.3. Décisions rendues par l'Organe de recours

1.3.1. Volume et répartition selon la nature des décisions

L'augmentation du nombre de recours introduits en 2025 s'est traduite par une hausse du nombre de décisions rendues par l'Organe de recours. Il convient toutefois de noter que ces décisions concernent en partie des dossiers introduits en 2024, et qu'une partie des recours introduits en 2025 seront traités en 2026. Ainsi, le nombre total de décisions rendues par l'Organe de recours est passé de 261 en 2024 à 357 en 2025, soit une progression de 37%.

Ces décisions concernaient :
- 164 habilitations de sécurité (46% du total),
- 177 avis de sécurité (49,5%),
- 16 attestations de sécurité (4,5%).

1.3.2. Réformations et désistements

Sur l'ensemble des recours examinés en 2025, l'Organe de recours a réformé[53] 47 décisions en matière d'habilitations de sécurité sur 164 (soit 28,7%), 6 décisions portant sur des attestations de sécurité sur 16 (soit 37,5%) et 62 avis de sécurité sur 177 (soit 35%). Ce résultat témoigne d'un contrôle effectif de l'Organe de recours qui procède à un examen approfondi conduisant, dans une proportion significative de cas, à la modification des décisions contestées.

Il convient par ailleurs de relever la part non négligeable de décisions donnant acte d'un désistement de recours : 12,3% de l'ensemble des décisions et avis rendus (44 sur 357), et plus précisément 17,7% des décisions rendues en matière d'habilitations de sécurité (29 sur 164). Un désistement traduit la volonté d'un requérant de mettre fin à la procédure. Cela intervient notamment lorsqu'un recours a été introduit pour absence de décision dans le délai légal et que l'autorité de sécurité ou de vérification rend finalement une décision pendant l'instance.

1.3.3. Délai de traitement des recours

En 2025, le délai moyen de traitement des dossiers s'est établi à 125,9 jours, soit un peu plus de 4 mois à compter de l'introduction du recours. Ce résultat illustre la capacité de l'Organe de recours à gérer un volume accru de dossiers par rapport à l'année précédente. Cette performance a notamment été rendue possible grâce au renforcement récent du personnel au sein du greffe (cf. *infra*) qui a permis de traiter efficacement le nombre croissant de recours tout en préservant la qualité des décisions et avis rendus.

Depuis mi-2025, l'Organe de recours siège toutes les semaines. Etant donné la pluralité des missions du Comité ainsi que des instances qui composent le siège de l'Organe de recours, il est difficilement envisageable d'organiser davantage qu'une audience par semaine.

53 Réformer une décision signifie que l'Organe de recours substitue à la décision initiale une nouvelle décision.

Il convient par ailleurs de préciser que le délai de traitement ne dépend pas uniquement de l'Organe de recours. Il est également conditionné par les (longs) délais dans lesquels les autorités de sécurité et de vérification transmettent les dossiers administratifs des requérants, point qui sera détaillé dans le paragraphe suivant.

1.4. Délai de réception des dossiers administratifs

Comme mentionné ci-dessus, l'Organe de recours est régulièrement confronté à une transmission tardive des dossiers administratifs par les autorités de vérification et de sécurité. Ces délais ont un impact direct sur la durée de traitement des recours, dans la mesure où l'Organe de recours ne peut statuer utilement qu'à la condition qu'il dispose (de l'intégralité) du dossier administratif.

En 2025, les délais de transmission des dossiers administratifs se répartissaient de la manière suivante :

a. En matière d'avis de sécurité :
- 48 dossiers ont été reçus dans le délai légal de 10 jours ;
- 71 dossiers ont été reçus dans un délai de 11 à 20 jours ;
- 37 dossiers ont été reçus dans un délai de 21 à 30 jours ;
- 77 dossiers ont été reçus dans un délai supérieur à 30 jours, dont 19 dossiers dans un délai de plus de 100 jours.

Au total, plus de 75% des dossiers administratifs en matière d'avis de sécurité ont été reçus en dehors du délai légal de 10 jours.

b. En matière d'habilitations de sécurité :
- 25 dossiers ont été reçus dans le délai légal de 15 jours ;
- 48 dossiers ont été reçus dans un délai de 16 à 30 jours ;
- 52 dossiers ont été reçus dans un délai de 31 à 99 jours ;
- 17 dossiers ont été reçus dans un délai de plus de 100 jours.

Au total, plus de 80 % des dossiers administratifs en matière d'habilitations de sécurité ont été reçus en dehors du délai légal de 15 jours. Ce retard participe à l'allongement des délais de traitement des recours par l'Organe de recours.

2. ÉVOLUTION DU CADRE JURIDIQUE ET DE LA JURISPRUDENCE

2.1. Nouvelle législation

La Loi du 2 juin 2024 modifiant la Loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé est entrée en vigueur le 1er février 2025. Les principales modifications sont présentées ci-dessous.

2.1.1. Disparition des attestations de sécurité

Alors qu'il existait initialement trois types de résultats de screening (les habilitations de sécurité, les attestations de sécurité et les avis de sécurité), la loi susmentionnée a supprimé les attestations de sécurité. Depuis le 1er février 2025, un avis de sécurité est désormais requis pour les fonctions et secteurs pour lesquels une attestation de sécurité était auparavant requise.

2.1.2. Modifications concernant les avis de sécurité

Parmi les modifications apportées par la loi précitée, l'article 36 de la Loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé (« loi classification ») introduit deux nouveaux types d'avis de sécurité positifs, à savoir l'avis de sécurité positif avec mise en garde individuelle et l'avis de sécurité positif avec avertissement administratif.

Un avis de sécurité positif avec mise en garde individuelle signifie que l'autorité ne dispose pas d'éléments suffisants pour émettre un avis négatif, mais qu'elle met en garde le requérant quant à la nécessité d'améliorer son comportement sur les points mentionnés.

Un avis de sécurité positif avec avertissement administratif est délivré lorsque le requérant n'a pas séjourné en Belgique durant les cinq années couvertes par la vérification de sécurité et que l'autorité ne dispose pas d'informations suffisantes à son sujet. Par ailleurs, depuis le 1er février 2025, il est également possible d'introduire un recours lorsque l'autorité de vérification n'a pas rendu d'avis de sécurité dans le délai légal.

2.2. Question préjudicielle posée à la Cour constitutionnelle

En 2024, l'Organe de recours a posé une question préjudicielle à la Cour constitutionnelle afin de savoir si les articles 17 et 18 du Code judiciaire, relatifs à l'exigence d'un intérêt né et actuel pour introduire un recours, étaient compatibles avec les articles 10 et 11 de la Constitution. Plus précisément, cette question portait sur la recevabilité d'un recours devant l'Organe de recours en cas de refus d'habilitation de sécurité lorsque le requérant n'avait pas préalablement contesté la rupture de son contrat devant la juridiction compétente.

Dans cette affaire, l'Autorité nationale de sécurité (ANS) avait refusé de renouveler l'habilitation de sécurité du requérant, employé au sein de l'OTAN, ce qui avait conduit à la résiliation de son contrat de travail.

Par son arrêt n°36/2025 du 27 février 2025, la Cour a estimé que l'exigence d'un intérêt né et actuel, c'est-à-dire en l'espèce que le requérant démontre avoir contesté la perte de son emploi, portait une atteinte disproportionnée au droit d'accès à un juge. Cette exigence privait également d'effet utile le recours spécifique prévu pour les décisions en matière d'habilitations de sécurité. La Cour a donc validé une interprétation de la loi permettant de saisir l'Organe de recours dès le refus ou le retrait d'une habilitation de sécurité, ou en cas d'absence de décision dans le délai prévu, sans condition

supplémentaire. L'arrêt consacre ainsi une interprétation large du droit de recours, en écartant toute exigence excessive d'intérêt à agir, afin de garantir l'effectivité du recours.

2.3. Recevabilité du recours et compétence du Conseil d'Etat vs de l'Organe de recours

La question de la compétence de l'Organe de recours s'est posée dans le cadre d'une affaire au sujet de laquelle la Section du contentieux administratif du Conseil d'Etat s'est prononcée dans son arrêt début septembre 2025.[54] Dans ce dossier, le requérant, agent contractuel pour la Commission européenne recruté afin de travailler dans un poste à l'étranger, avait sollicité une habilitation de sécurité de niveau « EU SECRET » requise pour l'exercice de cette fonction.

L'ANS a indiqué ne « pas pouvoir donner de suite favorable à cette demande », estimant que l'enquête de sécurité ne pouvait être réalisée et ainsi ne pas être capable de réunir les informations suffisantes pour apprécier si le requérant présentait les garanties requises. L'ANS invoquait notamment le fait que le requérant ait exercé des fonctions à l'étranger pendant la quasi-totalité de la période d'enquête et qu'il ne résidait plus en Belgique depuis de nombreuses années. La notification précisait qu'en cas de désaccord, le requérant pouvait introduire une requête en annulation de cette décision auprès du Conseil d'Etat.

L'avocate du requérant, doutant de la compétence du Conseil d'Etat, a, par mesure de précaution, introduit un recours auprès des deux instances. Elle soutenait qu'il s'agissait bien d'une décision de refus d'habilitation de sécurité.

Le Conseil d'Etat a confirmé cette analyse, estimant qu'en déclarant ne pas pouvoir donner de « suite favorable » à la demande d'habilitation de sécurité, l'ANS a de manière implicite mais certaine refusé l'octroi de cette habilitation. Or, l'article 4, §1er, L.Org.Recours attribue expressément à l'Organe de recours la compétence pour connaître des décisions de refus d'habilitations. Le Conseil d'Etat a donc jugé qu'il ne pouvait ni annuler, ni suspendre une telle décision. Le Conseil d'Etat a également précisé que les motifs invoqués par l'ANS, à savoir le séjour prolongé à l'étranger et l'absence de résidence en Belgique, n'y changeaient rien. Dès lors qu'il s'agit d'un refus, la compétence revient à l'Organe de recours, indépendamment des raisons avancées.

2.4. Impossibilité d'enquête

L' « impossibilité d'enquête » a été invoquée par l'ANS dans d'autres dossiers similaires. L'Organe de recours a en effet été saisi de plusieurs dossiers dans lesquels l'ANS considérait l'enquête de sécurité impossible au motif que le requérant résidait à l'étranger. Comme exposé *supra*, l'ANS contestait la compétence de l'Organe de recours au motif que l'acte attaqué ne constituait pas un « refus d'octroyer une habilitation », mais plutôt un simple constat de l'impossibilité d'enquêter.

54 Conseil d'Etat, Arrêt n°264.054 du 3 septembre 2025.

A la suite de l'arrêt précité du Conseil d'Etat, l'Organe de recours s'est déclaré compétent dans ces différents dossiers. Il a considéré que l'ANS ne pouvait invoquer de manière systématique une impossibilité d'enquêter dès que la partie requérante était engagée dans une carrière à l'étranger, alors même que la fonction concernée exige de séjourner à l'étranger.

L'Organe de recours a, dans le cadre de ces dossiers, rappelé que les services de renseignement et de sécurité disposaient d'une large compétence pour effectuer diverses démarches dans le cadre d'une enquête de sécurité, y compris en dehors du territoire belge.[55] Il considère par ailleurs qu'une autorité de sécurité doit fournir des efforts raisonnables pour mener son enquête. Par exemple, l'Organe de recours estime qu'il est possible de prendre en compte les évaluations professionnelles de la partie requérante, d'organiser un entretien avec elle, de considérer ses liens avec Belgique, de contacter l'officier de sécurité régional, ou encore d'envisager l'adoption de mesures de mitigation. Compte tenu de ce qui précède, l'Organe de recours a estimé qu'il était possible de mener une enquête dans ces différents dossiers.

2.5. Le screening comme mesure de ressources humaines dissimulée

L'Organe de recours constate que des screenings se soldent régulièrement par un résultat négatif pour des motifs non conformes aux dispositions légales. Il ressort des dossiers traités que, parfois, une habilitation de sécurité est refusée ou qu'un avis de sécurité négatif est émis sur la base de motifs qui ne constituent pas un danger pour l'ordre démocratique ou la sécurité nationale. Cela constitue une application incorrecte des dispositions légales en vigueur.

Une habilitation de sécurité n'est requise que si la personne concernée doit accéder à des informations classifiées. La personne concernée doit alors présenter des garanties suffisantes en matière d'intégrité, de loyauté et de discrétion. Une habilitation de sécurité ne peut être refusée que s'il existe des éléments concrets laissant penser que la personne concernée représente un risque pour la sécurité nationale. L'Organe de recours se doit de vérifier si la décision de l'autorité de sécurité respecte les critères légaux.

2.6. Le screening sur la base d'une décision réglementaire

Malgré une forte augmentation du nombre de screenings, l'Organe de recours doit également veiller à ce que ces screenings reposent toujours sur une base réglementaire. Ainsi, un screening a été effectué sur les participants à une séance d'information sur le thème « travailler au sein de la Police locale », qui s'est déroulée dans les locaux d'une zone de police locale. Lorsqu'il est saisi, l'Organe de recours vérifie en premier lieu sur quelle décision réglementaire repose la vérification effectuée. Or, dans le cas d'espèce, le screening était uniquement imposé pour les personnes appelées à exercer temporairement une mission ou une fonction dans les locaux de la Police locale. L'Organe de recours a estimé que la participation à une séance d'information ne relevait en aucun cas de la catégorie « exercice d'une fonction ou d'une mission ». La personne en question s'était donc vu refuser à tort

55 Voir articles 18 et 19 de la Loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé.

la participation à la séance d'information ; plus encore, *de facto*, tous les participants à la séance d'information avaient été indûment soumis à un screening.

Il va sans dire que, compte tenu notamment du nombre croissant de screenings, il convient de veiller en permanence à ce qu'ils soient effectués dans le respect de la loi. Il demeure essentiel de vérifier si un screening de sécurité est nécessaire ou non et si ce screening permet effectivement d'atteindre l'objectif pour lequel cet instrument est utilisé.

2.7. Application de l'article 5 §3 L.Org.Recours

Le respect des droits de la défense implique que le requérant doit pouvoir connaître la raison ou la motivation pour laquelle on lui refuse une habilitation de sécurité ou on lui délivre un avis de sécurité négatif. Il peut arriver que certaines informations ne puissent pas être divulguées au risque de porter atteinte à d'autres intérêts : informations personnelles concernant des tiers, fonctionnement des services de sécurité, déroulement d'une enquête judiciaire, protection des sources.

En vertu de l'article 5 § 3 L.Org.Recours, les autorités de sécurité ou les autorités de vérification peuvent demander à l'Organe de recours de ne pas autoriser le requérant ou son avocat à consulter certaines informations pour les raisons susmentionnées. Le cas échéant, il convient de mettre en balance les intérêts en présence afin de donner également au requérant une réelle possibilité de se défendre et de pouvoir contester de manière substantielle une décision ou un avis négatif. Concrètement, cela signifie que toutes les demandes de mise d'informations sous « embargo » ne sont pas systématiquement accordées.

3. RECOURS PORTÉS DEVANT D'AUTRES JURIDICTIONS

3.1. Cassation devant le Conseil d'Etat

En 2025, trois recours en cassation ont été introduits contre des décisions rendues par l'Organe de recours. Un dossier a été déclaré irrecevable en raison de l'absence de moyens recevables. Les deux autres dossiers étaient toujours en cours à la fin de l'année 2025. Enfin, un dossier introduit en 2024 a été rejeté en 2025 par le Conseil d'État. Le rejet du pourvoi en cassation a été motivé par l'absence de violation des dispositions légales. Le requérant en cassation avait invoqué une violation de son droit d'être entendu ainsi que de l'obligation de motivation. Ces deux moyens ont été rejetés.

3.2. Requête devant la Cour européenne des droits de l'Homme

Une requête a également été introduite devant la Cour européenne des droits de l'Homme. Cette dernière concerne un recours contre un avis de sécurité négatif.

Le requérant invoque l'article 6 de la Convention des droits de l'Homme, estimant que l'impossibilité d'accéder à des éléments de preuves déterminants soumis à l'Organe de recours ainsi que le caractère inadéquat de sa décision constituent une violation de son droit à un procès équitable. Il se prévaut également de l'article 8 de la Convention, soutenant que l'avis de sécurité négatif constitue une atteinte à sa vie privée, en particulier au regard de sa vie professionnelle. Le dossier était toujours en cours fin 2025.

4. ORGANISATION INTERNE ET FONCTIONNEMENT DU GREFFE

4.1. Organisation interne et effectifs

L'augmentation du nombre de recours introduits en 2025 (voir *supra*) a eu un impact direct sur l'organisation des audiences et sur la charge de travail de l'Organe de recours.

Depuis le printemps 2025, deux audiences par mois sont organisées pour les dossiers francophones, permettant l'examen de 12 à 15 dossiers par audience.

A partir de la mi-2025, en raison de la hausse significative des recours introduits en néerlandais, le même rythme de deux audiences mensuelles a été instauré pour les dossiers néerlandophones, avec un nombre équivalent de dossiers examinés.

L'Organe de recours représente une charge de travail particulièrement importante au sein du Comité R/I, alors même qu'il ne constitue qu'une parmi les nombreuses missions qui lui sont confiées. Pour faire face à l'augmentation du contentieux et au volume croissant de tâches administratives, deux collaborateurs ont été recrutés en septembre et octobre 2025 pour renforcer le greffe de l'Organe de recours. Ce renfort a permis de maintenir des délais de traitement raisonnables malgré l'intensification de l'activité contentieuse. Le traitement des dossiers mobilise actuellement l'équivalent de deux juristes (un francophone et un néerlandophone) et de quatre secrétaires à plein temps. La présidente et le conseiller y consacrent environ 20% de leur temps de travail.

4.2. Digitalisation et modernisation de la procédure

En 2025, une réflexion approfondie a été entamée, portant sur la digitalisation de la procédure de recours devant l'Organe de recours. L'objectif vise notamment à alléger la charge de travail du greffe et à faciliter l'introduction d'un recours pour les citoyens.

Ce projet implique une analyse fonctionnelle des différentes étapes de la procédure, un développement informatique ainsi qu'une révision des règles encadrant le dépôt et l'instruction des recours. Il s'agit d'un chantier de longue durée, qui se poursuivra en 2026, en raison des adaptations techniques et réglementaires nécessaires.

A terme, l'objectif est de permettre aux requérants de pouvoir opter pour une procédure électronique. Une telle évolution devrait réduire de manière significative le nombre d'envois recommandés effectués par l'Organe de recours et contribuer à diminuer les coûts qui y sont liés, actuellement estimés à environ 50 euros par dossier dans les cas les plus simples. La digitalisation offrirait également une meilleure traçabilité des échanges, une réduction des délais de transmission et une simplification du travail du greffe.

LA COOPERATION (INTER)NATIONALE

PARTAGER LES EXPERTISES

1. LES ÉCHANGES INTERNATIONAUX

A l'heure où les services de renseignement multiplient les échanges (y compris d'informations et de données) au-delà des frontières, le Comité R/I est convaincu de la nécessaire coopération, au niveau international, entre autorités de contrôle. Qu'elle prenne la forme de rencontres bilatérales ou de groupes de travail plus larges, cette coopération permet d'identifier les bonnes pratiques en matière de contrôle des services de renseignement et de déceler des pistes pour le renforcer et le maintenir à la hauteur des défis contemporains.

En 2025, l'intelligence artificielle, l'achat d'ensembles massifs de données (*bulk data*) et la Convention 108+ constituaient les sujets phares des forums internationaux auxquels a participé le Comité R/I.

Rencontre avec la *Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*, 2 avril 2025, Bruxelles

Une délégation de la *Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* (CTIVD) des Pays-Bas a été reçue au Comité R/I en avril 2025. La rencontre a été l'occasion d'échanger sur les spécificités propres à chaque institution mais également sur les défis communs auxquels elles font face. Parmi les sujets abordés, la lutte contre la criminalité organisée et l'achat d'ensembles massifs de données ont fait l'objet d'échanges approfondis. Cette visite a posé les fondations d'une collaboration renforcée entre les deux organes de contrôle.

European Intelligence Oversight Network, 20 mai 2025, Bruxelles

En 2025, le workshop du *European Intelligence Oversight Network* (EION)[56] était dédié à l'utilisation par les services de renseignement et de sécurité de données obtenues de sources commerciales. Les discussions ont permis de dresser un état des lieux de la réglementation et du contrôle concret de ces pratiques. La Convention 108+ et l'horizon qu'elle offre d'une coopération internationale renforcée entre autorités de contrôle ont également été évoqués.

Intelligence Oversight Working Group, 21-23 mai 2025, Copenhague

Une réunion *technical* de l'*Intelligence Oversight Working Group* (IOWG)[57] s'est tenue à Copenhague fin mai 2025. Après un tour de table des actualités de chaque institution, les participants ont échangé sur leur contrôle de l'usage de l'intelligence artificielle par les services de renseignement et de la gestion de leurs bases de données. Le volet technique était suivi d'une réunion *staff* lors de laquelle les membres de l'IOWG ont évoqué les défis rencontrés lors de leur contrôle. Il était par exemple

56 L'EION réunit des représentants des autorités de contrôle de Belgique, du Canada, du Danemark, de France, d'Allemagne, de la Lituanie, des Pays-Bas, de Norvège, de Serbie, de Suède, de Suisse, du Royaume-Uni et des Etats-Unis.

57 Dans le cadre d'IOWG se réunissent les autorités de contrôle de Belgique, du Danemark, des Pays-Bas, de Norvège, du Royaume-Uni, de Suisse, de Suède et du Canada.

question de la gestion des ressources humaines, des délais parfois importants pour la conduite des enquêtes, de la stratégie de communication ou encore de l'accès aux services de renseignement.

Intelligence Oversight Working Group, 4-5 novembre 2025, Zurich

Les membres de l'IOWG se sont une nouvelle fois réunis fin 2025, à Zurich. Lors de ce rendez-vous, les débats ont notamment porté sur l'utilisation de cryptomonnaies par les services de renseignement, la gestion du savoir et de l'expertise au sein des organes de contrôle ou encore la formation de leur personnel. Les réunions *technical* et *staff* étaient suivies d'une réunion *Chair* où l'autorité de contrôle canadienne, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR – NSIRA), jusqu'à présent membre observateur, a été formellement admise comme membre à part entière de l'IOWG. Suite aux constats posés lors des réunions de mai et novembre 2025, deux groupes de travail ont été créés : le groupe de travail *AI Oversight* est dédié à l'usage (et son contrôle) de l'intelligence artificielle dans le contexte de la sécurité nationale et le groupe de travail *Oversight Gap* se penche sur les pistes de solutions pour une coopération internationale entre autorités de contrôle.

Séminaire « 'National Security' and the Politics of Security Screenings in a Globalized World », 5 novembre 2025, Oslo

En novembre 2025, l'expertise du Comité a été sollicitée dans le cadre d'un séminaire dédié à la problématique des screenings de sécurité à la *Olso Metropolitan University* (Oslomet). Il était notamment question des défis liés à des enquêtes de sécurité menées au niveau national dans un monde globalisé, ainsi que de la méthodologie utilisée par les services de renseignement pour la qualification de personnes.

European Intelligence Oversight Conference, 5-6 novembre 2025, Zurich

En novembre 2025, le Comité R/I a également assisté à la *European Intelligence Oversight Conference* (EIOC). Créé en 2018, l'EIOC se veut offrir un espace de rencontres et de discussions pour les autorités de contrôle et la société civile. En 2025, les échanges étaient notamment axés autour des ensembles massifs de données et des lacunes en matière de contrôle des services de renseignement et de sécurité.

International Intelligence Oversight Forum, 18-19 novembre 2025, Austin

En 2025, l'*International Intelligence Oversight Forum* (IIOFF) a eu lieu à Austin, Texas. Organisées autour de la thématique du « Contrôle du renseignement dans des environnements de sécurité complexes », les présentations portaient notamment sur les relations entre autorités de contrôles et services contrôlés, l'utilisation d'outils d'intelligence artificielle dans le cadre de la sécurité natio-

nale ainsi que la Convention 108+.[58] Le Comité a profité de sa présence à Austin pour rencontrer les membres du Strauss Center de l'Université du Texas, centre de recherche dédié au droit et à la sécurité internationale.

Rencontre avec la *Toetsingscommissie Inzet Bevoegdheden*, 27 novembre 2025, Bruxelles

Le Comité R/I a accueilli une délégation de la *Toetsingscommissie Inzet Bevoegdheden* (TIB) à Bruxelles. Aux Pays-Bas, cette commission est chargée du contrôle *a priori* des méthodes mises en œuvre par l'*Algemene Inlichtingen- en Veiligheidsdienst* (AIVD) et du *Militaire Inlichtingen- en Veiligheidsdienst* (MIVD). Lors de cette rencontre, les deux institutions ont évoqué leur obligations légales et usages en matière de communication, l'utilisation de l'intelligence artificielle par les services de renseignement ou encore le contrôle interne au sein de ces services.

2. LA COMMUNAUTÉ BELGE DU CONTRÔLE

Outre la coopération internationale, le Comité investit également dans les contacts et échanges avec les partenaires belges. Garantir le contrôle efficace des services de renseignement et de sécurité impose une coopération étroite entre les acteurs de la « communauté du contrôle » qui dépasse le seul Comité R/I.

2.1. Réunions communes avec le Comité P

L'article 52 L.Contrôle prévoit qu'au minimum deux réunions se tiennent annuellement entre le Comité R/I et le Comité P. En 2025, les Comités se sont réunis à deux reprises, en juillet et décembre. Les Comités ont discuté de l'état d'avancement de plusieurs dossiers communs, notamment le projet de révision d'un protocole d'accord sur l'exercice des compétences d'autorités de contrôle pour le traitement des données à caractère personnel ainsi que les dossiers et le fonctionnement de l'Organe de recours.

En parallèle, de nombreux échanges ont eu lieu avec le Comité P plus spécifiquement dans le cadre d'enquêtes de contrôle communes et du traitement conjoint de plaintes.

2.2. Plateforme Droits humains

Depuis 2015, toutes les institutions dotées d'un mandat en matière de droits humains ont pris l'engagement d'échanger des pratiques et méthodes de travail, d'examiner des questions communes

58 Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel.

et de promouvoir la coopération mutuelle.[59] Ces échanges s'organisent au sein de la Plateforme de concertation Droit humains.

En 2025, sept réunions ont été organisées sous la présidence du *Vlaams Mensenrechteninstituut* puis de l'Institut Fédéral pour la Protection et la Promotion des Droits Humains (IFDH). Lors de ces réunions, les discussions ont notamment porté sur l'accord de gouvernement fédéral, les soins de santé mentale en prison, la crise de l'accueil, le Règlement européen sur l'Intelligence artificielle et plus largement les défis de l'usage de l'intelligence artificielle par les services publics ou encore les développements politiques concernant la Cour européenne des droits de l'homme.

59 Protocole d'accord du 13 janvier 2015 entre les institutions exerçant partiellement ou entièrement un mandat d'institution chargée du respect des droits de l'homme.

FONCTIONNEMENT INTERNE

UNE ÉQUIPE RENFORCÉE

LA COMPOSITION DU COMITÉ R/I

Vanessa Samain et Séverine Merckx ont poursuivi l'exercice de leur mandat respectif de présidente et de membre francophone du Comité R/I. Linda Schweiger a été remplacée par Filip Vanneste, conseiller à la Cour d'appel d'Anvers, qui a prêté serment le 22 avril 2025 comme membre néerlandophone. Lors de la séance plénière de la Chambre des représentants du 6 novembre 2025, il a été reconduit pour un nouveau mandat de six ans.[1]

Dirigé par Frederic Verspeelt, le Service d'enquêtes était composé de sept commissaires-auditeurs. L'administration, sous la direction du greffier Frédéric Givron, a été renforcée grâce au recrutement d'un secrétaire, d'une employée, d'un juriste et d'une *Chief Information Security Officer* (CISO). Fin 2025, le personnel administratif comptait vingt-deux membres.

UNE RÉORGANISATION INTERNE

Pensée en concertation avec les membres du personnel, une réorganisation de la structure interne du Comité a été opérée dès janvier 2025. A côté des métiers de support (secrétariat, informatique, comptabilité, ressources humaines), l'administration est désormais organisée en deux sections principales, la section *Legal* en charge des questions et analyses juridiques et la section *Perspective & Analysis* comme centre de documentation et d'expertise. Des groupes de travail (GT) transversaux, réunissant des collègues de différents services au sein du Comité, ont à cette occasion été mis sur pied en vue de favoriser une approche multidisciplinaire des missions et responsabilités du Comité (GT Méthodes particulières de recueil de données, GT Communication interne et externe, GT Horizon 2030, etc.).

A travers cette nouvelle organisation, le Comité souhaitait clarifier les rôles et responsabilités de chaque équipe, notamment suite au renforcement des effectifs. La réforme entendait également répondre à plusieurs recommandations formulées par la Cour des Comptes dans son audit de 2024.

Cette réorganisation a fait l'objet d'une première évaluation à l'occasion de deux mises au vert, organisées respectivement en juin 2025 pour les membres du Service d'enquêtes et en octobre 2025 pour le personnel administratif. Ces séminaires hors site ont également permis de faire émerger des pistes concrètes pour la définition de nouveaux processus de travail. Les discussions ont aussi plus largement nourri la construction du futur plan stratégique du Comité R/I.

1 A cette occasion, Vinciane Boon et Isabelle Goes ont été nommées respectivement première et deuxième membres suppléantes francophones du Comité R/I.

UNE NOUVELLE IDENTITÉ VISUELLE

En 2025, le Comité a engagé une refonte de son identité visuelle. Cette démarche s'inscrit dans une volonté de renforcer la confiance, de souligner le professionnalisme et de refléter les valeurs et principes fondamentaux qui guident l'action du Comité. Légalité, intégrité, indépendance, transparence et rigueur : ces principes, piliers du fonctionnement du Comité, méritent une image qui les exprime et les renforce.

En tant qu'institution à dotation de la Chambre des représentants, le Comité s'adresse, au quotidien, aux parlementaires et responsables politiques. Ceux-ci ne sont toutefois pas l'unique « public cible » du Comité, dont les produits alimentent également plus largement la communauté du contrôle, incarnée par les partenaires institutionnels, la société civile ou encore la presse. Surtout, le Comité se veut résolument orienté vers le citoyen. En raison de ses missions complexes et multiples, menées en périphérie du confidentiel secteur de la sécurité nationale, il reste toutefois méconnu du grand public. Essentielles dans un Etat de droit, les activités du Comité peuvent pourtant avoir une influence directe sur les (droits des) citoyens – à travers, par exemple, le traitement de plaintes. La nouvelle identité visuelle du Comité vise donc également à renforcer sa visibilité et celle du contrôle des services de renseignement.

A travers ce logo, plusieurs métaphores traduisent l'identité du Comité. La métaphore de l'arbre symbolise une organisation enracinée, au fil de son histoire, dans un socle solide de valeurs. Le tronc incarne la stabilité et la fiabilité tandis que les branches illustrent la diversité de ses missions. Les multiples missions du Comité s'exercent de manière autonome, mais restent indissociables.

La référence discrète aux couleurs nationales fait écho aux principes démocratiques sur lesquels repose l'Etat belge. Elle rappelle la responsabilité du Comité d'agir de manière indépendante, impartiale et transparente, dans l'intérêt de chaque citoyen.

Ensemble, ces éléments graphiques composent une empreinte digitale unique, symbole de l'identité propre du Comité en tant qu'organe *sui generis*. Cette empreinte traduit la singularité, l'authenticité et la fiabilité de l'institution, tout en rappelant l'importance de la confidentialité et de la rigueur qui guide ses missions.

LA COMMISSION D'ACCOMPAGNEMENT PARLEMENTAIRE

Le Président de la Chambre, Peter De Roover (N-VA), assure la présidence 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 d'accompagnement). En 2025, en étaient membres avec voix délibérative Paul Van Tigchelt (Anders), Sammy Mahdi (cd&v), Stefaan Van Hecke (Ecolo-Groen), Benoît Lutgen (Les Engagés), Denis Ducarme

(MR), Benoît Piedboeuf (MR), Peter Buysrogge (N-VA), Christoph D'Haese (N-VA), Maaike De Vreese (N-VA), Khalil Aouasti (PS), Eric Thiébaut (PS), Greet Daems (PVDA-PTB), Francesca Van Belleghem (VB), Marijke Dillen (VB) et Brent Meuleman (Vooruit).

Dans le courant de l'année 2025, deux réunions de la Commission ont eu lieu au cours desquelles ont été discutés une enquête de contrôle, le rapport d'activités 2024, des dossiers en cours ainsi que le fonctionnement interne du Comité R/I.

L'OUVERTURE À L'EXPERTISE EXTERNE

Le Comité R/I veille à nourrir les réflexions internes autour des défis contemporains en matière de renseignement et de sécurité ou de contrôle démocratique. A cette fin, le Comité sollicite notamment l'intervention d'experts externes, invités à apporter leurs éclairages lors de *lunch* thématiques.

En 2025, deux séances ont été organisées. En juin, Bernard Siman (Institut Egmont/VUB) a présenté un exposé sur la « guerre hybride » et les transformations des pratiques de guerre et de paix. La seconde séance a accueilli en septembre le président du Comité de coordination du renseignement et de la sécurité, Pascal Petry, Conseiller à la Police fédérale, pour une présentation du fonctionnement concret de cette plateforme centrale dans l'architecture de sécurité belge.

BUDGET

Le budget 2025 du Comité R/I a été fixé à 6.393.778 €, ce qui représente une augmentation de 1,6% par rapport à 2024, correspondant à l'indexation et à l'évolution barémique du personnel.

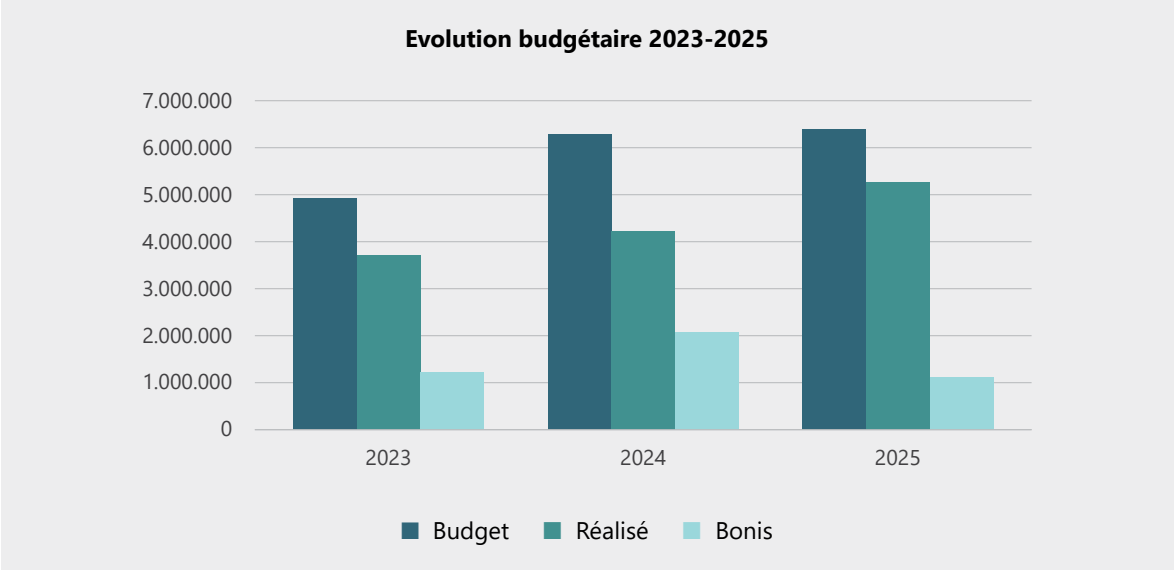
Le financement accordé par la Chambre des représentants se compose comme suit : 81% au titre du budget de dotation, seul apport en trésorerie net, et 19% de boni 2023. Ce financement est l'unique source de financement du Comité et permet de couvrir l'ensemble des activités du Comité.

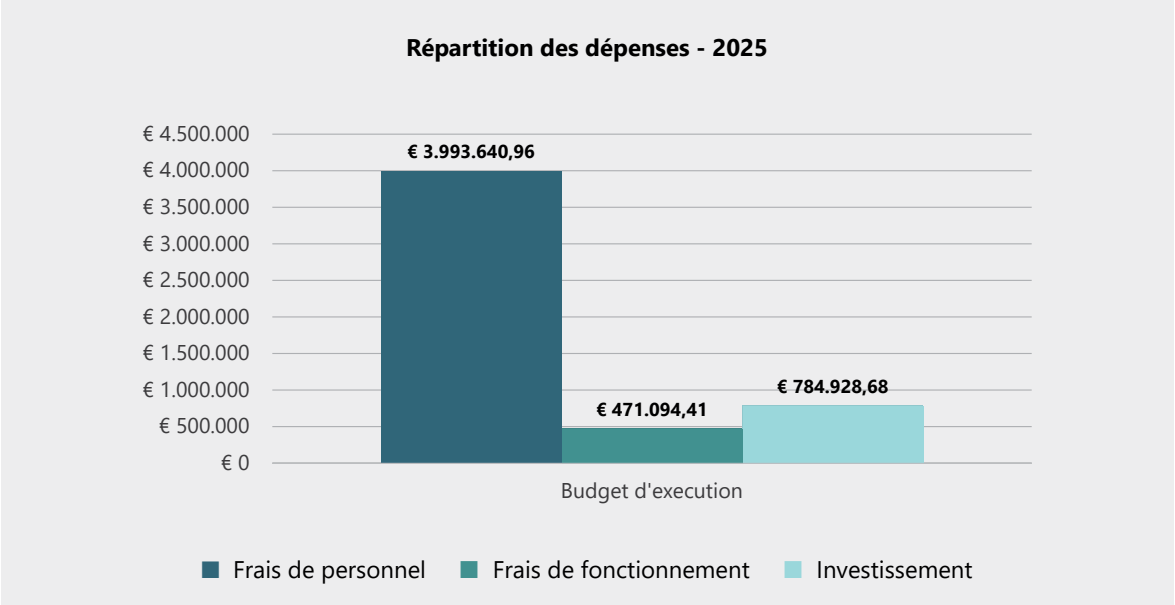
L'exécution du budget 2025 a produit un résultat comptable ou boni de 1.125.013 €, représentant la différence entre le budget approuvé et les dépenses constatées. Le boni comptable se répartit à part égale entre les frais de personnel et les frais de fonctionnement. Le dégagement d'un boni conséquent peut s'expliquer par deux facteurs.

- Le Comité a sollicité un financement exceptionnel sur trois ans, débuté en 2024, pour la digitalisation de ses processus et le renouvellement de ses infrastructures informatiques. La mise en œuvre de ce projet est soumise aux contrôles de sécurité inhérents à la nature des activités du Comité (les nécessaires habilitations de sécurité pour les firmes et le personnel octroyées au terme d'enquêtes de sécurité de neuf mois en moyenne) ainsi qu'à la recherche de l'optimalisation des ressources. L'identification de fournisseurs potentiels, des contrats-cadres disponibles, le contrôle des offres et l'attributions des missions s'en trouvent dès lors souvent retardés, empêchant la liquidation complète des crédits disponibles.

› Au cours des dernières années, l'augmentation des missions de contrôles historiques du Comité, la création de nouvelles missions résultants de modifications législatives, ainsi que l'augmentation de la charge liée à la gestion de l'Organe de recours, ont conduit le Comité à procéder au recrutement de nouveaux collaborateurs. Sur les exercices 2023, 2024 et 2025, plusieurs recrutements ou remplacements ont été initiés. La longueur du processus de recrutement, de l'obtention des habilitations de sécurité requises, auxquelles s'ajoute un préavis éventuel, peut conduire à un délai de plus d'un an entre l'appel à candidature et l'entrée en fonction du membre du personnel. Ce délai vient automatiquement nourrir le résultat comptable de l'année où le recrutement est en cours. Le Comité est attentif à cet enjeu et travaille à réduire, pour les paramètres qui relèvent de sa responsabilité, la durée du processus de recrutement.

Il est donc attendu que l'entrée en fonction des nouveaux collaborateurs au cours des années 2026, voire 2027, ainsi que la finalisation du projet de digitalisation, conduiront à un rééquilibrage du budget approuvé et des dépenses constatées et à la réduction du boni.





LE PROCESSUS DE DIGITALISATION

Alors que son infrastructure informatique devenait obsolète, le Comité R/I a obtenu fin 2023 un budget spécifique de la Chambre des représentants en vue d'un projet de digitalisation d'envergure lui permettant de moderniser son fonctionnement.

Suite aux importants investissements en matériels et logiciels informatiques (*hardware* et *software*) réalisés en 2024, les projets de 2025 se sont focalisés sur la digitalisation des processus de travail. En particulier, la modernisation du fonctionnement du greffe de l'Organe de recours permettra l'allègement des tâches administratives. En parallèle, le Comité finalise le développement d'une bibliothèque numérique permettant une gestion moderne et intuitive de sa documentation.

Une solution de sécurité matérielle a été installée afin de permettre le transfert unidirectionnel de données entre deux réseaux. Concrètement, le transfert de fichiers du réseau connecté à internet vers le réseau sécurisé du Comité est désormais presque instantané, dans le respect strict des normes de sécurité.

Ces développements informatiques sont d'une importance capitale pour maintenir une affectation équilibrée des ressources du Comité au regard de l'ensemble de ses missions. Ils offrent en outre aux membres du personnel des outils modernes, flexibles et collaboratifs, tout en garantissant un niveau de sécurité adéquat.

Différents projets ont par ailleurs été initiés pour moderniser le réseau classifié du Comité et une *Chief Information Security Officer* (CISO) a pris ses fonctions.

Le site internet de l'Organe de recours, géré par le Comité, a également été retravaillé en 2025. Son contenu a été adapté à la suite des importantes modifications législatives successives en matière d'habilitations et d'avis de sécurité. Le Comité disposera quant à lui d'un nouveau site internet en 2026.

ABRÉVIATIONS

ANS	Autorité nationale de sécurité
APD	Autorité de protection des données
BDC T.E.R.	Banque de données commune
CCRS	Comité de coordination du renseignement et de la sécurité
C.O.C.	Organe de contrôle de l'information policière
Comité P	Comité permanent de Contrôle des services de police
Comité R/I	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
CSIL	Cellules de sécurité intégrale locales
DPO	*Data protection officer*
IFDH	Institut fédéral pour la protection et la promotion des droits humains
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
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
MPR	Méthodes particulières de renseignement
OCAM	Organe de coordination pour l'analyse de la menace
PFCECT	Plateforme commune *Counter Extremism & Counter Terrorism*
PSNR	Plan stratégique national de renseignement
SGRS	Service Général du Renseignement et de la Sécurité
Stratégie T.E.R.	Note stratégique Extrémisme et Terrorisme
TFL	Task forces locales
UE	Union européenne
VSSE	Sûreté de l'État